



Contract # AR2481

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

Emergent, LLC

Name		
<u>8219 Leesburg Pike, Suite 300</u>		
Address		
<u>Vienna</u>	<u>VA</u>	<u>22182</u>
City	State	Zip

LEGAL STATUS OF CONTRACTOR

☐	Sole Proprietor
☐	Non-Profit Corporation
☐	For-Profit Corporation
☒	Partnership
☐	Government Agency

Contact Person James Flint Phone # 703-635-2616 Email jflint@emergent360.com
Vendor # VC205734 Commodity Code # 81110

2. GENERAL PURPOSE OF CONTRACT: Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed.
3. PROCUREMENT: This contract is entered into as a result of the procurement process on Bid# CH16012.
4. CONTRACT PERIOD: Effective Date: 04/17/2017 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation # CH16012, Contractor must re-certify its qualifications each year.
5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on Sales of Services invoiced during the calendar quarter.
6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Price Schedule
ATTACHMENT D: Contractor's Response to Solicitation # CH16012
ATTACHMENT E: Applicable Manufacturer Terms and Conditions
- Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.**
8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
 - Utah State Procurement Code, Procurement Rules, and Contractor's response to Bid # CH16012.
9. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

Paul D. Kohler 04/24/2017
Contractor's signature Date

Paul D. Kohler, Executive Vice President
Type or Print Name and Title

STATE

[Signature] 4/27/17
Director, Division of Purchasing Date

Solomon Kingston

Division of Purchasing Contact Person

801-538-3228

Telephone Number

801-538-3882

Fax Number

skingston@utah.gov

Email

(Revision 16 June 2016)



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

- (1) A Participating Entity's Participating Addendum¹ ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits² to the Master Agreement;
- (3) The Solicitation;
- (4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
- (5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be agreed to by the parties in writing and attached to this Master Agreement as an Exhibit or Attachment.

¹ A Sample Participating Addendum will be published after the contracts have been awarded.

² The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and SaaS, as well as Applicable Manufacturer Terms and Conditions.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Affiliates means any entity that controls, is controlled by or is under common control with the Contractor.

Applicable Laws means local, state or federal laws or regulations, to the extent applicable to the relevant Services provided by Contractor, including, but not limited to such laws and regulations regarding data privacy and security.

Applicable Manufacturer means any provider of commercially-available cloud solutions approved, as applicable, by the Lead State and/or the applicable Participating Entity, whose Products/Services are available for purchase under this Master Agreement. For purposes of clarification, a formal amendment shall not be required to add an Applicable Manufacturer, but for convenience, Exhibit I in Attachment E to the Master Agreement will be updated to include approved, additional Applicable Manufacturers.

Applicable Manufacturer Terms and Conditions means the specific manufacturer terms and conditions attached as Exhibits in Attachment E to this Master Agreement, which are current as of the date of this Master Agreement, but are subject to change. The then current version of the Applicable Manufacturer Terms and Conditions shall apply at the time of purchase and will be provided to the Purchasing Entity in accordance with the applicable Participating Addendum. For clarification purposes, Applicable Manufacturer Terms and Conditions include support terms and SLAs (as such term is defined hereinafter).

Confidential Information is non-public proprietary or confidential information that is received by Contractor or Purchasing Entity in connection with this Master Agreement and is marked or identified at the time of disclosure as “confidential” or that a reasonable person should understand to be confidential, including, but not limited to: (1) any Purchasing Entity’s records, (2) personnel records, (3) information concerning individuals, (4) trade secrets, software, source code, know how, techniques, and processes, and (5) financial information, excluding pricing under this Master Agreement.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and Affiliates who are providing the Products/Services agreed to under the Master Agreement.

Data means information, whether in oral or written (including electronic) form, created by or originating with a Participating Entity or Purchasing Entity, and information that is the output of any computer processing, or other electronic manipulation, of information that was created by or originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Master Agreement, excluding metadata, and subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions.

Data Breach means any actual or reasonably suspected non-authorized access to or

acquisition of computerized Non-Public Data or Purchasing Entity Personal Data that materially compromises the security, confidentiality, or integrity of the Non-Public Data or Purchasing Entity Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Purchasing Entity Personal Data, and subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions.

Data Center means the Applicable Manufacturer data center housing the servers and other equipment necessary to provide the basic functionality of the Services, as described in the applicable service description. Other data centers used to store records regarding maintenance and support (even where such records contain Purchasing Entity's Data), shall not be considered Data Centers.

Data Categorization means the process of risk assessment of Data. See also "High Risk Data", "Moderate Risk Data" and "Low Risk Data".

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event (except for the expiration of a subscription based Service), and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity's software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating and is subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Products/Services under this Master Agreement and billing Customers directly for such Products/Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("High Impact Data").

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined as the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has

control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information and is subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, or other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter

into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate or that subsequently executes a Participating Addendum. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Purchasing Entity Personal Data means (i) data alone or in combination, that is the output of any computer processing or other electronic manipulation, or otherwise created in the course of Purchasing Entity's use of the Services provided under this Master Agreement, that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record, (ii) is stored and processed by the Services, and (iii) is subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions. Personal information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person. Purchasing Entity Personal Data does not include metadata generated by Data collection tools.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Price List means the then current Applicable Manufacturer commercial price list for the Products/Services.

Product means any deliverable under this Master Agreement, including Services, hardware, software, maintenance, support, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium, which is stored and processed by the Services, and is subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health

care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI does not include network centric information such as IP addresses or MAC addresses.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Purchase Order or Order means a written or electronic order from Purchasing Entity to Contractor for the Products/Services to be provided under this Master Agreement.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Purchasing Entity's Personal Data the Contractor believes could reasonably result in a Data Breach.

Service Level Agreement (SLA) means the Applicable Manufacturer Terms and Conditions which specify the standards to which the manufacturer agrees to adhere and by which it measures the level of service for its Services. The then current version of the manufacturer's SLA shall apply at the time of purchase and will be provided to the Purchasing Entity at such time.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user- specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written document or contract agreed by the parties in a form based upon the Applicable Manufacturer's requirements that describes the Services to be performed, inclusive of the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: The initial term of this Master Agreement is for ten

(10) years with no renewal options. However, the term of any Purchase Order shall be set forth in the Purchase Order. The Purchase Order term shall commence on the effective date of the Purchase Order and shall continue for a period of one (1) year, or such other multiyear period as set forth in the Purchase Order. Such term will be renewed automatically for successive one (1) year terms unless either party notifies the other of its intent to terminate at least sixty (60) days prior to the expiration of the then current term. In addition, if a State desires the term of a Purchase Order to extend beyond the term of the Master Agreement, then the State shall expressly allow such action in a Participating Addendum, in which case the term of a Purchase Order may then extend beyond the term of the Master Agreement and the applicable Participating Addendum, if the Purchase Order term, including options, was specifically stated in the Purchase Order.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written agreement of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State; provided, however, that Contractor may assign, sell, transfer or sublet rights or delegate responsibilities to an Affiliate, or a third party in connection with a merger, reorganization, reincorporation, or consolidation, or a third party that acquires all or substantially all of its assets or a majority or controlling interest of the Contractor.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction for new Purchase Orders for the Products/Services provided under this Master Agreement following approved Price List updates. Price List updates will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination for Convenience: Unless otherwise stated, this Master Agreement may be terminated by either party for convenience upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 60 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending Purchase Orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Products/Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance of an applicable Service Level Agreement in association with any Purchase Order, obligations under Termination and Suspension of

Service in accordance with the Applicable Manufacturer's Terms and Conditions, and any responsibilities arising out of a Security Incident or Data Breach in accordance with the Applicable Manufacturer's Terms and Conditions. Termination of Purchase Orders for Services for convenience may only occur if expressly permitted by the applicable Purchase Order, and may result in termination fees as set forth in the applicable Purchase Order. Termination of the Master Agreement due to Contractor default may be immediate if defaults cannot be reasonably cured as allowed per Default and Remedies terms.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Each party hereto acknowledges that it and its employees or agents may, in the course of providing or receiving a Product under this Master Agreement, be exposed to or acquire information that is confidential to Contractor, the Applicable Manufacturer, Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by a receiving party shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by the receiving party) publicly known; (2) is furnished by Contractor or Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in the receiving party's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than the disclosing party without the obligation of confidentiality, (5) is disclosed with the written consent of the disclosing party or; (6) is independently developed by employees, agents or subcontractors of receiving party who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. The receiving party shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. The receiving party shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. The receiving party shall use commercially reasonable efforts to assist the disclosing party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, the receiving party shall advise the disclosing party, and as applicable the Participating Entity, and the Lead State, immediately and if permitted by applicable law, if the receiving party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and the receiving party shall at its expense cooperate with the disclosing party in seeking injunctive or other equitable relief in the name of the disclosing party against any such person. Except as directed by the disclosing party, the receiving party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at the disclosing party's, the receiving

party shall turn over to the disclosing party all documents, papers, and other matter in the receiving party's possession that embody Confidential Information. Notwithstanding the foregoing, the receiving party may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. The receiving party acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to the disclosing party that is inadequately compensable in damages. Accordingly, the disclosing party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. The receiving party acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of the disclosing party and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

e. Notwithstanding the foregoing, damages attributable to a Data Breach and/or Security Incident shall be subject to the Section of the Master Agreement titled "Limitation of Liability."

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement, including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or the applicable Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

- (1) Nonperformance of contractual requirements; or
- (2) A material breach of any term or condition of this Master Agreement; or
- (3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; provided that Contractor shall not be deemed to have made a certification, representation or warranty simply by providing the Applicable

Manufacturer Terms and Conditions; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement; or

(6) Any default or invoked right to terminate specified in the Applicable Manufacturer Terms and Conditions.

(7) Undisputed fees under a Purchase Order which are not paid when due and payment has not been received within thirty (30) days after notice from Contractor of such past due payment.

b. Upon the occurrence of an event of default, the non-defaulting party to this Master Agreement or the applicable Participating Addendum shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which the defaulting party shall have an opportunity to cure the default. The non-defaulting party shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the non-defaulting party, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate the non-terminating party's liability for damages.

c. If the defaulting party is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, the defaulting party shall be in breach of its obligations under this Master Agreement and the non-defaulting party, as applicable, shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement, or the applicable Participating Addendum or Purchase Order or portions thereof; and

(3) In the case of a Participating Entity, suspend Contractor from being able to respond to future bid solicitations; and

(4) In the case of a Participating Entity, suspend Contractor's performance on affected Purchase Orders; and

(5) Withhold payment or the provision of affected Services until the default is remedied; and

(6) Exercise any additional remedies set forth in the Applicable Manufacturer Terms and Conditions.

d. Rights upon Termination or Expiration.

(1) Upon termination of the Master Agreement, any Participating Addendum, or a Purchase Order, Purchasing Entity shall pay Contractor, as applicable, for all applicable undisputed fees due for Products/Services provided up to the date of such termination and/or termination charges (if applicable) owed under the

affected Purchase Order, at the agreed-upon prices, fees, and expense reimbursement rates; provided that written notice is provided to Contractor regarding any disputed fees for Products/Services and the parties work in good faith to resolve any such dispute.

(2) Termination of a particular Service will not impact any other Service or the Master Agreement, which will remain in full force and effect. Purchase Orders for a particular Service placed and accepted under this Master Agreement or any Participating Addendum prior to expiration of the contract term (even if involving a multi-year commitment) remain valid and binding in accordance with the contract terms for the term stated therein.

(3) In the event of any termination pursuant to this section, and unless otherwise required by law or court of competent jurisdiction, the Lead State, Participating Entities and Purchasing Entities shall all remain obligated to comply in perpetuity with the provisions of the Applicable Manufacturer's Terms and Conditions for the applicable Service, and provisions of this Master Agreement regarding Confidential Information.

e. Unless otherwise specified in the Participating Addendum or Purchase Order, in the event of a default under a Participating Addendum or Purchase Order, a non-defaulting party shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum or Purchase Order. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a non-defaulting party under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, identified in Contractor's response to the Solicitation as responsible for the administration of this Master Agreement, in writing within 10 calendar days of the change.

12. Force Majeure: Except for the obligation to pay monies due and owing, the Contractor, Lead State, Participating Entity, or Purchasing Entity, as applicable, shall not be in default by reason of any failure in performance of this Master Agreement, Participating Addendum, or Purchase Order, which is outside of its reasonable control and without its fault or negligence. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party on its part. The obligations and rights of the excused party shall be extended on a day-by-day basis for the time period equal to the period of the excusable delay.

13. Indemnification

a. Subject to Section 44 of this Master Agreement and to the extent not prohibited by law, the Contractor shall defend third party claims or causes or actions asserted against

NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees (each an "Indemnified Party") and indemnify the Indemnified Party from and against any resultant damages agreed to in settlement by the Contractor or awarded by a court of final adjudication, including reasonable attorneys' fees and related costs, for any death, injury, or damage to tangible property (not including lost or damaged data) to the extent caused by the negligence or intentional misconduct of the Contractor or its employees, relating to the performance under the Master Agreement.

The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of such a claim. The Contractor shall have control over the defense and settlement of any such claim. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense.

b. Indemnification – Intellectual Property. Subject to Section 44 of this Master Agreement, if a third party makes a claim against NASPO, NASPO ValuePoint, the Lead State, a Participating Entity, or a Purchasing Entity, along with its officers, agents, and employees ("Indemnified Party"), that the Product furnished by Contractor and used by the Purchasing Entity, infringes the third party's United States copyright, United States patent, or other Intellectual Property rights ("Intellectual Property Claim"), Contractor will defend the Indemnified Party against the Intellectual Property Claim and indemnify the Indemnified Party from the damages, liabilities, costs and expenses awarded by the court to the third party claiming infringement or the settlement agreed to by Contractor, if the Indemnified Party does the following:

- i. notify Contractor promptly in writing, not later than thirty (30) days after the Indemnified Party receives notice of the Intellectual Property Claim (or sooner if required by applicable law);
- ii. give Contractor sole control of the defense and any settlement negotiations;
- and
- iii. give Contractor the information, authority, and assistance Contractor needs to defend against or settle the Intellectual Property Claim.

(1) However, the Contractor will not indemnify the Indemnified Party and the obligations under this section shall not apply if an Indemnified Party (a) alters the Product or uses it outside the scope of the use identified in the Applicable Manufacturer's Terms and Conditions, (b) uses a version of the Product which has been superseded, if the Intellectual Property Claim could have been avoided by using an unaltered current version of the Product which was provided to the Purchasing Entity, or (c) continues to use the applicable Product after the end of the license to use the Product. Contractor will not indemnify the Indemnified Party to the extent that an Intellectual Property Claim is based upon any information, design, specification, instruction, software, data, or material not furnished by Contractor. Contractor will not indemnify the Indemnified Party to the extent that an Intellectual Property Claim is

based upon the combination of the Product with any other product, services, system or method not provided by Contractor. Contractor will not indemnify the Indemnified Party to the extent that an Intellectual Property Claim is based on third party content or any material from a third party portal or other external source that is accessible to the Indemnified Party within or from the Services (e.g., a social media post from a third party blog or forum, a third party Web page accessed via a hyperlink, etc.). Contractor will not indemnify the Indemnified Party for infringement caused by the Indemnified Party's actions against any third party if the Services as delivered to the Purchasing Entity and used in accordance with the terms of the Applicable Manufacturer Terms and Conditions and the Purchasing Entity's applicable Purchase Order, would not otherwise infringe any third party Intellectual Property rights. Contractor will not indemnify the Indemnified Party for any Intellectual Property Claim(s) known to the Indemnified Party at the time the Product is purchased.

(2) If Contractor believes or it is determined that any portion of the Product may have violated a third party's Intellectual Property rights, Contractor may choose to either modify the Product to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for continued use, or if these alternatives are not commercially reasonable, Contractor may end the license for, and require return of, the applicable Product and refund the fees the Purchasing Entity paid for such Product. If such return materially affects Contractor's ability to meet its obligations under the relevant Purchase Order, then Contractor, may, at its option and upon thirty (30) days prior written notice, terminate the Purchase Order. Contractor's right to end the Purchase Order in accordance with this paragraph shall not apply if the Purchasing Entity authorizes or consents to use of the Product, and in such cases, Contractor shall have no obligation to indemnify or other liability whatsoever, to the Indemnified Party or to third parties for infringement.

(3) THIS SECTION STATES THE INDEMNIFIED PARTY'S SOLE AND EXCLUSIVE REMEDY AND CONTRACTOR'S ENTIRE LIABILITY FOR INTELLECTUAL PROPERTY CLAIMS UNDER THIS MASTER AGREEMENT. THIS INDEMNITY OBLIGATION AND REMEDY ARE GIVEN TO PURCHASING ENTITY SOLELY FOR ITS BENEFIT AND IN LIEU OF, AND CONTRACTOR DISCLAIMS, ALL WARRANTIES, CONDITIONS, AND OTHER TERMS OF NON-INFRINGEMENT, EXCEPT AS SET FORTH IN SECTION 31(A) OF THIS MASTER AGREEMENT, WITH RESPECT TO ANY PRODUCT OR SERVICE.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum or Purchase Order.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be as follows:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than \$1 million per occurrence/\$2 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions
	Minimum Insurance Coverage
Low Risk Data	\$2,000,000
Moderate Risk Data	\$5,000,000
High Risk Data	\$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of \$1,000,000 per occurrence and \$1,000,000 in the aggregate, written on a claims made form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Unless otherwise set forth in a Participating Addendum,

the Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations. Also, Contractor and/or the Applicable Manufacturer shall not be required to secure any specific additional licensing from a governmental authority that the Applicable Manufacturer does not hold as of the effective date of this Master Agreement. Additionally, if a change in applicable law after the effective date requires a change in the scope of the Services, at Purchasing Entity's option, Contractor will be entitled to either terminate the Services or recover any reasonable additional costs it may incur by virtue of the need to change the Services to comply with any changes to such laws, and in such case this Master Agreement, Participating Addendum, and applicable Purchase Order will be modified accordingly. Notwithstanding the foregoing, if there are any changes to any applicable law (including any decisions or interpretations by a relevant court or governmental authority relating thereto) that would restrict Contractor and/or the Applicable Manufacturer from performing the Services ("Restrictions"), the parties will meet to discuss and agree, in good faith, how to address the Restrictions. This may include revision of the scope of Services to implement a mutually agreeable workaround or the elimination of affected Services from the scope to address the Restrictions. Furthermore, and notwithstanding anything contained in the Master Agreement to the contrary, modifications which Contractor and/or the Applicable Manufacturer deems necessary to comply with specifications, changed safety standards or governmental regulations, to make the Services non-infringing with respect to any patent, copyright, or other proprietary interest, or to otherwise improve the Services may be made at any time by Contractor and/or the Applicable Manufacturer without prior notice to or consent of Purchasing Entity or NASPO ValuePoint, unless Services are materially altered, and such altered Service shall be deemed fully conforming.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering and Pricing:

a. Purchasing Entity may place Purchase Orders for the various Products/Services offered by Contractor with either Contractor, a Fulfillment Partner, or an Affiliate. The delivery and/or provision of any such Products/Services, if accepted by Contractor, shall be subject to the terms and conditions set forth in this Master Agreement, including those attached hereto as Attachment E, as well as the then-current Service descriptions for such Service offerings.

b. Master Agreement Order and Purchase Order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

c. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

d. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of Products/Services contemplated by this Master Agreement.

e. Contractor, Fulfillment Partner, or Affiliate, as applicable, shall not begin delivering and/or providing Products/Services without a valid Purchase Order or other appropriate commitment document compliant with the law of the Purchasing Entity.

f. Purchase Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

g. All Purchase Orders pursuant to this Master Agreement, at a minimum, shall include:

- (1) The Products/Services being delivered;
 - (2) The place/location and requested time of delivery/start date for commencement of the Services;
 - (3) A billing address;
 - (4) The name, phone number, and address of the Purchasing Entity representative;
 - (5) The price per unit or other pricing elements consistent with this Master Agreement and the Contractor's proposal;
 - (6) A ceiling amount of the Purchase Order for Products/Services being ordered;
- and
- (7) The Master Agreement identifier and the Participating State contract identifier.

- (8) Tax exempt certifications, if applicable; and
- (9) Additional information required by the Applicable Manufacturer.

h. All communications concerning administration of Purchase Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Purchase Order.

i. Purchase Orders must be placed pursuant to this Master Agreement or the applicable Participating Addendum prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

j. Notwithstanding the expiration or termination of this Master Agreement or the applicable Participating Addendum, Contractor agrees to perform in accordance with the terms of any Purchase Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Purchase Orders placed after the expiration or termination of this Master Agreement or the applicable Participating Addendum. Purchase Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

k. Contractor reserves the right to subcontract to a third party organization, subject to any subcontracting requirements in the applicable Participating Addendum, including Fulfillment Partners or Affiliates to provide Products/Services to Purchasing Entity, or to require that purchases be made through Fulfillment Partners or Affiliates; provided that acceptance of Purchase Orders, invoicing and/or receipt of payments will only be handled by and through Contractor or its authorized Fulfillment Partners or Affiliates. In addition, any such subcontract shall not relieve Contractor of any of its obligations under this Agreement.

l. Any contingencies on Purchasing Entity's Purchase Orders are not binding upon Contractor. The terms and conditions of this Master Agreement and applicable Participating Addendum prevail, regardless of any additional or conflicting terms on the Purchase Order, or other correspondence from Purchasing Entity to Contractor and any additional or conflicting terms are deemed rejected by Contractor, unless the parties have expressly agreed to such terms in writing. Mere acceptance or processing of a Purchase Order containing such terms shall not constitute such express consent.

m. Prices for Products/Services shall be those specified in Contractor's then current Price List, less any applicable Price List category or individual Service based discount(s) authorized in writing by Contractor to Purchasing Entity and valid at the time of acceptance of the Purchase Order by Contractor (a "Discount Authorization"), or in accordance with an applicable, valid written price quotation, if any, submitted by Contractor to Purchasing Entity for such Products/Services.

n. All stated prices are exclusive of any taxes, fees, and duties or other similar amounts, however designated, and including without limitation value added, sales and withholding taxes, which are levied or based upon such prices, charges, or upon this Master Agreement. Purchasing Entity will pay sales and use taxes, if any, imposed on the Products/Services acquired under this Master Agreement, or furnish proof of its tax-exempt status upon request. Contractor will pay all other taxes based on Contractor's income or gross receipts, or personal property taxes levied or assessed on Contractor's personal property. In the event that the Purchasing Entity is exempt from property and sales taxes, it will not be charged same.

20. Participants and Scope

a. Contractor may not deliver Products/Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Purchase Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Purchase Orders, governing law and venue, Purchase Order requirements, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. Purchase Order or contract) used by the Purchasing Entity to place the Purchase Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific Products/Services procured through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office.

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. Financial obligations of Participating States are limited to the Purchase Orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of

political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell Products/Services obtained under this Master Agreement.

21. Payment: Unless otherwise stipulated in the Participating Addendum, payment is due net 30 days following the date of invoice. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of an invoice, if disputed in good faith, upon written notice to Contractor. If, at any time, Purchasing Entity is delinquent in payment, or is otherwise in breach of this Master Agreement, Contractor may, without prejudice to other rights, withhold Services and/or require Purchasing Entity to prepay for further Services. Any sum not paid by Purchasing Entity when due shall bear interest until paid at a rate of one percent per month (12 months per annum) on the outstanding balance, or the maximum legal rate, whichever is less. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions, Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Purchasing Entity Data to fulfill Contractor's obligations under this Agreement. Subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions Contractor shall not access a Purchasing Entity's user accounts or Purchasing Entity Data, except in the course of Data Center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may disclose Purchasing Entity's Data to its Affiliates subject to the

confidentiality terms of this Master Agreement, who have a need to know related to performance under this Master Agreement. Contractor is responsible for any breach of these provisions by such Affiliates. Contractor may not share a Purchasing Entity's Data with any other third party without the Purchasing Entity's express written consent.

Subject to further refinement in accordance with the Applicable Manufacturer Terms and Conditions, Contractor will ensure that, prior to being granted access to Purchasing Entity Data, Contractor Staff who perform work under this Agreement have successfully completed instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Purchasing Entity Data they will be handling.

23. Operations Management: Applicable Manufacturer shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in accordance with the Applicable Manufacturer Terms and Conditions.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, excluding metadata, which may be used in accordance with the Applicable Manufacturer Terms and Conditions. Unless otherwise set forth in the Applicable Manufacturer Terms and Conditions, Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. Unless otherwise set forth in the Applicable Manufacturer Terms and Conditions, no information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Unless otherwise set forth in the Applicable Manufacturer Terms and Conditions, Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement, the applicable Participating Addendum and Purchase Orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees ("Audit Purpose"). Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, at such party's own expense, to audit, inspect, examine, copy and/or transcribe

Contractor's books, documents, papers and records directly pertinent to this Master Agreement, the applicable Participating Addendum, or Purchase Orders placed by a Purchasing Entity under it for the Audit Purpose. This right shall survive for a period of six (6) years following termination of this Master Agreement or final payment for any Purchase Order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms of this Master Agreement regarding payments.

Such access will be 1) with at least ten (10) business days advance written notice, (2) conducted during normal business hours, 3) shall not unduly interrupt or interfere with Contractor's normal business operations, and 4) in the event that such audit is conducted by a third party, such third party shall, prior to conducting such audit, execute a confidentiality agreement for the benefit of Contractor in a form reasonably satisfactory to Contractor.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments which are documented as a result of such audit as inconsistent with the terms of the Master Agreement or Purchase Orders or Contractor will bill the applicable Lead State, Participating Entity, or Purchasing Entity for any underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and any express language in the Master Agreement that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit for the Audit Purpose relative to the applicable Participating Addendum. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense, subject to the limitations set forth in subsection (a) above.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with the Contractor's response to the Solicitation by the Lead State.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state requesting the

additional fee. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be calculated by multiplying 0.25% against the "Net Purchase Price" paid by the Purchasing Entity. The "Net Purchase Price" is defined as the purchase price for Services authorized for sale under this Master Agreement, and excluding sales, use, or other applicable taxes, surcharges, or like fees, to the extent applicable to a Purchase Order.

For Services, Contractor will pay the administrative fee during the quarter the Purchase Order was accepted by Contractor or the Fulfillment Partner, as applicable, or in accordance with the agreed upon delivery schedule in a Purchase Order or subscription pricing arrangement. For example, for a three (3) year Services subscription paid one (1) year in advance, the administrative fee for the portion allocated to the first year of the subscription will be due in the quarter the initial sale is reported, while the administrative fee allocated to the second and third years will be due in the quarters that the subsequent transactions are reported, respectively.

28. System Failure or Damage: To the extent that system failure or damage is caused by Contractor or its Services, the Contractor agrees to use commercially reasonable efforts to restore or assist in restoring the system to operational capacity in accordance with the Applicable Manufacturer Terms and Conditions.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity a license to use the API if permitted and as set forth in the Applicable Manufacturer Terms and Conditions.

30. Data Privacy: When required by a specific Purchase Order issued under this Master Agreement or a Participating Addendum, and accepted by the Contractor, the Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to accepting an Purchase Order from a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the Purchase Order or Statement of Work.

31. Warranty and Disclaimer: Unless otherwise set forth in a PA, the Contractor warrants the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Products/Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, Purchase Orders issued against Participating Addendums, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation

by the Lead State.

c. Unless otherwise set forth in the Applicable Manufacturer Terms and Conditions, the Contractor will not interfere with a Purchasing Entity's access to and use of the Products/Services it acquires from this Master Agreement for which Contractor has received payment in full.

d. Unless otherwise set forth in the Applicable Manufacturer Terms and Conditions, the Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

e. Unless otherwise set forth in the Applicable Manufacturer Terms and Conditions, the Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor will use technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc. as set forth in the Applicable Manufacturer Terms and Conditions.

f. **Warranty for Professional Services.** Contractor shall perform Professional Services (defined as consulting, implementation, database/application administration, systems engineering and configuration services, training and other services) in a workmanlike manner in accordance with generally accepted industry standards. Unless otherwise agreed to in a Statement of Work, Purchasing Entity must notify Contractor in writing of any failure to so perform within ten (10) business days after the performance of the applicable portion of Professional Services.

Contractor's entire liability and Purchasing Entity's sole remedy for Contractor's failure to so perform shall be for Contractor to, at its option, (i) correct such failure; (ii) reperform the service, or (iii) terminate the applicable Statement of Work and refund that portion of any fees received that correspond to such failure to perform.

g. **THE WARRANTIES SET FORTH ABOVE AND IN THE APPLICABLE MANUFACTURER TERMS AND CONDITIONS ARE THE ONLY EXPRESS WARRANTIES PROVIDED BY CONTRACTOR. CONTRACTOR EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESSED, STATUTORY OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, AND ANY AND ALL WARRANTIES IMPLIED FROM CUSTOM, USAGE IN TRADE OR COURSE OF DEALING.**

FOR ANY BREACH OF THE ABOVE WARRANTIES, PURCHASING ENTITY'S EXCLUSIVE REMEDY AND CONTRACTOR'S ENTIRE LIABILITY SHALL BE AS SET FORTH IN THE MASTER AGREEMENT OR PARTICIPATING ADDENDUM.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement or the applicable Participating Addendum. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at an additional cost to the Purchasing Entity, if available and in accordance with the Applicable Manufacturer Terms and Conditions. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create and agree in writing upon a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as mutually agreed upon by the parties.

33. Waiver of Breach: Failure of the Contractor, Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Contractor, Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Contractor, Lead State, or Participating Entity, of any default, right or remedy under this Master Agreement or Participating Addendum, or by the Contractor or a Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any Products/Services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or the applicable Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment: The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Purchase Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for Products/Services entered into during the duration of an Purchase Order and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and Products/Services established per each written agreement). No new leases, maintenance or other agreements for Products/Services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of Products/Services, subscriptions, and other service agreements, shall not be considered as “new.”

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Purchase Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the Solicitation, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Purchase Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. Notwithstanding any of the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's or the Applicable Manufacturer's intellectual property or proprietary rights.

e. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh

Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Products/Services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Products/Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the Products/Services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Purchase Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Purchase Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Purchase Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Purchase Orders placed under this master agreement.

41. Government Support: Unless otherwise set forth in a PA, no support, facility space, materials, special access, personnel or other obligations on behalf of the Participating States or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at <http://www.naspo.org/WNCPO/Calculator.aspx>. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment F.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the Solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report. Notwithstanding the above, sales to employees are not allowed under the Master Agreement, unless the Applicable Manufacturer permits such sales, and the parties hereto mutually agree in writing to allow such sales to employees under the Master Agreement.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and

otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. Entire Agreement: This Master Agreement, along with any attachment, and/or other documents expressly incorporated into this Master Agreement by reference, contains the entire understanding of the parties hereto with respect to the subject matter of this Master Agreement and replaces any prior oral or written communications between the parties, unless a term is modified by mutual written agreement in a Participating Addendum with a Participating Entity or in an Purchase Order placed by the Purchasing Entity or in an amendment to this Master Agreement. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted, except for those terms which are attached to and incorporated and made part of this Master Agreement in accordance with Attachment E.

44. Limitation of Liability:

A. CONTRACTOR'S MAXIMUM LIABILITY AND THE SOLE AND EXCLUSIVE REMEDY UNDER THIS MASTER AGREEMENT FOR ANY CLAIM, LOSS, DAMAGE OR LIABILITY ARISING OUT OF, RELATED TO, OR CONNECTED WITH THE APPLICABLE PURCHASE ORDER, AND WHETHER BASED UPON DEFAULT, OR OTHER LIABILITY SUCH AS BREACH OF CONTRACT, WARRANTY, NEGLIGENCE, MISREPRESENTATION OR OTHERWISE, SHALL IN NO CASE EXCEED, IN THE AGGREGATE, DIRECT DAMAGES IN AN AMOUNT EQUAL TO TWO (2) TIMES THE TOTAL AMOUNTS ACTUALLY PAID TO THE CONTRACTOR FOR THE SERVICES UNDER THE APPLICABLE PURCHASE ORDER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM LESS ANY REFUNDS OR CREDITS RECEIVED BY THE PURCHASING ENTITY FROM CONTRACTOR UNDER SUCH PURCHASE ORDER, OR ONE MILLION DOLLARS (\$1,000,000), WHICHEVER IS GREATER.

B. NOTWITHSTANDING THE ABOVE, NEITHER THE CONTRACTOR NOR THE PURCHASING ENTITY SHALL BE LIABLE FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT OR SPECIAL DAMAGES OF ANY KIND, WHICH MAY RESULT DIRECTLY OR INDIRECTLY FROM SUCH PERFORMANCE, INCLUDING, WITHOUT LIMITATION, DAMAGES RESULTING FROM DATA, DATA USE, LOSS OF USE, LOSS OF DATA, LOSS OF REVENUE OR PROFITS (EXCLUDING FEES UNDER THE APPLICABLE PURCHASE ORDER), INTERRUPTION OF BUSINESS, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR LOSS OF PROFIT BY THE PURCHASING ENTITY, THE CONTRACTOR, OR BY OTHERS, UNDER ANY CAUSE OR ACTION (INCLUDING WITHOUT LIMITATION CONTRACT, TORT, OR STRICT LIABILITY) ARISING FROM OR OUT OF THIS MASTER AGREEMENT OR A PURCHASING ENTITY'S PURCHASE ORDER, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

The limitations of liability in this Section will not apply to claims for infringement, bodily injury, or tangible personal property damage.

45. Severability: In the event that part of or one or more terms of this Master Agreement becomes or is declared to be illegal or otherwise unenforceable by any court of competent jurisdiction, each such part or term shall be null and void and shall be deemed deleted from this Master Agreement. All remaining terms of this Master Agreement shall remain in full force and effect. Notwithstanding the foregoing, if this paragraph is invoked and, as a result, the value of this Master Agreement is materially impaired for either party, as determined by such party in its sole discretion, then the affected party may terminate this Agreement or the applicable Participating Addendum by written notice with immediate effect to the other.

46. Survival: The following sections shall survive the expiration or earlier termination of this Master Agreement Sections 2 (Definitions), 7 (Termination), 8 (Confidentiality, Non-Disclosure, and Injunctive Relief), 10 (Default and Remedies), 12 (Force Majeure), 21 (Payment), 31 (Warranty and Disclaimer), 32 (Transition Assistance), 33 (Waiver of Breach), 37 (Governing Law and Venue), 43 (Entire Agreement), 44 (Limitation of Liability), 45 (Severability), 46 (Survival), 47 (Notices), and the parts of Attachment E that expressly state that they shall survive, shall survive the termination or expiration of this Master Agreement.

47. Notices: Notwithstanding anything contained in this Master Agreement to the contrary, all notices required or permitted under this Master Agreement will be in writing and will be deemed given: (a) when delivered personally; (b) when sent by confirmed facsimile or electronic mail; (c) three (3) days after having been sent by registered or certified mail, return receipt requested, postage prepaid (or six (6) days for international

mail); or (d) one (1) day after deposit with a commercial express courier specifying next day delivery (or two (2) days for international courier packages specifying 2-day delivery), with written verification of receipt. All communications will be sent to the addresses set forth in this Master Agreement or such other address as may be designated by a party by giving written notice to the other party pursuant to this section. Notwithstanding the above, notices regarding general changes in pricing, policies, or programs may also be made by email or fax.

48. Use of Services: All use of the Services will comply with the Applicable Manufacturer Terms and Conditions set out in Attachment E, which is incorporated herein by reference.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. **Security Incident Reporting Requirements:** The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

b. **Breach Reporting Requirements:** If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted

and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

- a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.
- b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.
- c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

- a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing
- b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.



Attachment B – Scope of Services Awarded to Contractor

Identification of Service Models Matrix

Offerors must complete the following form to identify the service models your firm offers under this RFP. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer, including the Categorization of Risk that you have the ability to store and secure. This document is to provide purchasing entities and eligible users a quick snap shot of the cloud solutions your firm provides.

Cloud Service Provider	Service Model(s)	Deployment Model(s)	Risk Category
Amazon Web Services	IaaS, PaaS, SaaS	Private, Community, Public, Hybrid	High, Moderate, or Low
Microsoft Azure	IaaS, PaaS, SaaS	Private, Community, Public, Hybrid	High, Moderate, or Low
IBM/SoftLayer	IaaS	Private, Public, Hybrid	Moderate or Low



Emergent, LLC
8219 Leesburg Pike
Suite 300
Vienna, VA 22182
Main: (703) 288-4556
Fax: (703) 288-4287
www.emergent360.com

NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

State of Utah
Solicitation Number CH16012

Cost Proposal

Closing Date: March 10, 2016
Closing Time: 1:00 pm MNT

This proposal includes information that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to this offeror or quoter as a result of or in connection with the submission of this information, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this proposal or quotation if it is obtained from another source without restriction. The information subject to this restriction is contained on sheets with the following disclosure legend: "Use or disclosure of information contained on this sheet is subject to the restriction on the title page of this proposal."



Table of Contents

Section Title: Cost Proposal	1
Discounts: Cloud Service Providers	1
Labor Rates: Professional Services (Years 1 - 5).....	2
Labor Rates: Professional Services (Years 6 - 10).....	2

Section Title: Cost Proposal**Discounts: Cloud Service Providers**

Cloud Service Provider	Discount from List Price	Minimum Threshold
Amazon Web Services	2.5%	None
Micosoft Azure	8%	None
IBM/SoftLayer	2.5%	None
	3%	\$3,000
	4%	\$5,000
	5%	\$15,000
	7.5%	\$25,000
	10%	\$100,000

Labor Rates: Professional Services (Years 1 - 5)

LCAT	Year 1	Year 2	Year 3	Year 4	Year 5
Senior Solution Architect	\$250.00	\$257.50	\$265.23	\$273.18	\$281.38
Solution Architect	\$235.00	\$242.05	\$249.31	\$256.79	\$264.49
Senior Principal Consultant	\$270.00	\$278.10	\$286.44	\$295.04	\$303.89
Principal Consultant II	\$255.00	\$262.65	\$270.53	\$278.65	\$287.00
Principal Consultant I	\$240.00	\$247.20	\$254.62	\$262.25	\$270.12
Senior Consultant	\$210.00	\$216.30	\$222.79	\$229.47	\$236.36
Staff Consultant	\$185.00	\$190.55	\$196.27	\$202.15	\$208.22
Associate Consultant	\$160.00	\$164.80	\$169.74	\$174.84	\$180.08
Program Manager	\$228.00	\$234.84	\$241.89	\$249.14	\$256.62
Project Manager II	\$227.00	\$233.81	\$240.82	\$248.05	\$255.49
Project Manager I	\$180.00	\$185.40	\$190.96	\$196.69	\$202.59
Contracts Administrator	\$160.00	\$164.80	\$169.74	\$174.84	\$180.08
Subject Matter Expert II	\$300.00	\$309.00	\$318.27	\$327.82	\$337.65
Subject Matter Expert I	\$282.00	\$290.46	\$299.17	\$308.15	\$317.39

Labor Rates: Professional Services (Years 6 - 10)

LCAT	Year 6	Year 7	Year 8	Year 9	Year 10
Senior Solution Architect	\$289.82	\$298.51	\$307.47	\$316.69	\$326.19
Solution Architect	\$272.43	\$280.60	\$289.02	\$297.69	\$306.62
Senior Principal Consultant	\$313.00	\$322.39	\$332.07	\$342.03	\$352.29
Principal Consultant II	\$295.61	\$304.48	\$313.62	\$323.03	\$332.72
Principal Consultant I	\$278.23	\$286.57	\$295.17	\$304.02	\$313.15
Senior Consultant	\$243.45	\$250.75	\$258.27	\$266.02	\$274.00
Staff Consultant	\$214.47	\$220.90	\$227.53	\$234.35	\$241.38
Associate Consultant	\$185.48	\$191.05	\$196.78	\$202.68	\$208.76
Program Manager	\$264.31	\$272.24	\$280.41	\$288.82	\$297.49
Project Manager II	\$263.16	\$271.05	\$279.18	\$287.56	\$296.18
Project Manager I	\$208.67	\$214.93	\$221.38	\$228.02	\$234.86
Contracts Administrator	\$185.48	\$191.05	\$196.78	\$202.68	\$208.76
Subject Matter Expert II	\$347.78	\$358.22	\$368.96	\$380.03	\$391.43
Subject Matter Expert I	\$326.92	\$336.72	\$346.82	\$357.23	\$367.95



Emergent, LLC
8219 Leesburg Pike
Suite 300
Vienna, VA 22182
Main: (703) 288-4556
Fax: (703) 288-4287
www.emergent360.com

NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

State of Utah
Solicitation Number CH16012

Technical Proposal

Closing Date: March 10, 2016
Closing Time: 1:00 pm MNT

This proposal includes information that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to this offeror or quoter as a result of or in connection with the submission of this information, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this proposal or quotation if it is obtained from another source without restriction. The information subject to this restriction is contained on sheets with the following disclosure legend: "Use or disclosure of information contained on this sheet is subject to the restriction on the title page of this proposal."

Table of Contents

Section Title: RFP Signature Page	1
Requirement 5.1 (M) SIGNATURE PAGE.....	1
Section Title: Executive Summary	2
Substantiation.....	2
Depth and Breadth of Proposed Solutions	2
Information Provided	3
Section Title: Mandatory Minimums.....	4
Requirement 5.2 (M) COVER LETTER	5
Requirement 5.2.1	6
Requirement 5.2.2	6
Requirement 5.2.3	6
Requirement 5.2.4	7
Requirement 5.2.5	7
Requirement 5.2.6	10
Requirement 5.3 (M) ACKNOWLEDGEMENT OF AMENDMENTS	11
Requirement 5.5 (M) GENERAL REQUIREMENTS	11
Requirement 5.5.1	11
Requirement 5.5.2	11
Requirement 5.5.3	11
Requirement 5.5.4	12
Requirement 5.7 RECERTIFICATION OF MANDATORY MINIMUMS AND TECHNICAL SPECIFICATIONS.....	12
Section Title: Business Profile.....	13
Requirement 6.2 (M)(E) SCOPE OF EXPERIENCE.....	14
Requirement 6.3 (M) FINANCIALS	14
Requirement 6.4 (E) GENERAL INFORMATION	15
Requirement 6.4.1	15
Use and Acceptance of Solutions in the Marketplace	17
Requirement 6.4.2	18
6.5 (E) BILLING AND PRICING PRACTICES	19
Requirement 6.5.1 and 6.5.2	19
Total Cost of Ownership (TCO) Calculator	21
Requirement 6.5.3	21
Requirement 6.6 (E) SCOPE AND VARIETY OF CLOUD SOLUTIONS.....	22
Scope and Variety: Amazon Web Services.....	22
Scope and Variety: Microsoft Azure.....	23

Scope and Variety: VMware vCloud Air	25
Scope and Variety: SoftLayer	27
Requirement 6.7 (E) BEST PRACTICES.....	28
Best Practices: Amazon Web Services.....	28
AWS: Built-In Security Features.....	29
AWS: Visibility into Data, Performance, and Resource Usage	30
AWS: Third-Party Security Tools.....	30
Best Practices: Microsoft Azure.....	31
Microsoft Azure: Security Design and Operations.....	31
Microsoft Azure: Visibility, Compliance, Data Security and Threat Protection	32
Best Practices: VMware vCloud Air	33
VMware vCloud Air: Cloud Computing Security.....	33
VMware vCloud Air: Visibility, Compliance, Data Security and Threat Protection	34
Best Practices: SoftLayer	35
SoftLayer: Multi-Layer Security Strategy	35
SoftLayer: Visibility, Compliance, Data Security and Threat Protection	35
Section Title: Organization Profile	38
Requirement 7.1 (ME) CONTRACT MANAGER.....	38
Requirement 7.1.1	38
Requirement 7.1.2	38
Requirement 7.1.3	39
Section Title: Technical Response.....	41
FedRAMP: Applicable Requirements, Standards, and Guidance.....	41
Requirement 8.1 (M)(E) TECHNICAL REQUIREMENTS	42
Requirement 8.1.1	42
Requirement 8.1.2	43
Requirement 8.1.2.1	43
Requirement 8.1.2.2	44
Requirement 8.1.2.3	45
Requirement 8.1.2.4	45
Requirement 8.1.2.5	46
Requirement 8.1.3	46
Requirement 8.1.4	49
Requirement 8.1.5	49
Requirement 8.2 (E) SUBCONTRACTORS.....	50
Requirement 8.2.1	50
Requirement 8.2.2	50

Requirement 8.3 (E) WORKING WITH PURCHASING ENTITIES	51
Requirement 8.3.1	51
ISO/IEC 27001	52
NIST SP 800-61 <i>Computer Security Incident Handling Guide</i>	54
Requirement 8.3.2	55
Requirement 8.3.3	56
Requirement 8.3.4	56
Requirement 8.3.5	57
Requirement 8.3.6	57
Requirement 8.4 (E) CUSTOMER SERVICE.....	57
Requirement 8.4.1	57
Customer Service: Service Level Agreements	58
Customer Service: Support Plans	58
Amazon Web Services: Support Plans	58
Microsoft Azure: Support Plans	59
VMware vCloud Air: Support Plans	60
SoftLayer: Free Support	61
Requirement 8.4.2	62
Requirement 8.5 (E) SECURITY OF INFORMATION	62
Requirement 8.5.1	62
Requirement 8.5.2	63
Requirement 5.6.4	63
Requirement 8.6 (E) PRIVACY AND SECURITY	64
Requirement 8.6.1	64
Requirement 8.6.2	64
Requirement 8.6.3	66
Requirement 8.6.4	68
Requirement 8.6.5	69
Requirement 8.6.6	70
Requirement 8.6.7	71
Requirement 8.6.8	71
Requirement 8.6.9	71
Physical Security	71
Virtual Control	72
Requirement 8.6.10	72
Requirement 8.7 (E) MIGRATION AND REDEPLOYMENT PLAN	73
Requirement 8.7.1	73

Requirement 8.7.2	74
Requirement 8.8 (E) SERVICE OR DATA RECOVERY	74
Requirement 8.8.1	74
Requirement 8.8.2	74
Requirement 8.9 (E) DATA PROTECTION	76
Requirement 8.9.1	76
Requirement 8.9.2	77
Requirement 8.9.3	77
Requirement 8.10 (E) SERVICE LEVEL AGREEMENTS	78
Requirement 8.10.1	78
Requirement 8.10.2	78
Requirement 8.11 (E) DATA DISPOSAL	78
Requirement 8.12 (E) PERFORMANCE MEASURES AND REPORTING	79
Requirement 8.12.1	79
Requirement 8.12.2	80
Requirement 8.12.3	80
Requirement 8.12.4	80
Requirement 8.12.6	80
Requirement 8.12.7	80
Requirement 8.12.8	80
Requirement 8.12.9	81
Requirement 8.12.10	81
Requirement 8.12.11	81
Requirement 8.13 (E) CLOUD SECURITY ALLIANCE	81
Requirement 8.14 (E) SERVICE PROVISIONING	82
Requirement 8.14.1	82
Requirement 8.14.2	82
Requirement 8.15 (E) BACK UP AND DISASTER PLAN	82
Requirement 8.15.2 and 8.15.3	82
Requirement 8.15.4	82
Requirement 8.16 (E) SOLUTION ADMINISTRATION	84
Requirement 8.16.1	84
Requirement 8.16.2	86
Requirement 8.16.3	87
Requirement 8.16.4	87
Requirement 8.16.5	87
Requirement 8.17 (E) HOSTING AND PROVISIONING	88



Requirements 8.17.1 and 8.17.2	88
Requirement 8.17.3	89
Requirement 8.18 (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE).....	89
Requirements 8.18.1, 8.18.2, 8.18.3.....	89
Requirement 8.19 (E) INTEGRATION AND CUSTOMIZATION.....	90
Requirements 8.19.1 and 8.19.2	90
Requirement 8.20 (E) MARKETING PLAN.....	92
Commitment to NASPO/ValuePoint	93
Marketing the NASPO/ValuePoint Master Agreement	93
Sales Enablement	94
Requirement 8.21 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS	94
Requirement 8.22 (E) SUPPORTING INFRASTRUCTURE	95
Requirement 8.22.1 and 8.22.2	95
Requirement 8.23 (E) ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE	95
Section Title: Confidential, Protected or Proprietary Information.....	97
Section Title: Exceptions and/or Additions to the Standard Terms and Conditions.....	98
Section Title: Cost Proposal	104

Tables and Figures

Table 1: NIST Cloud Computing Service and Deployment Models. Emergent's proposed cloud solutions meet the requirements of NIST SP 800-145.	7
Table 2: Service Model Subcategories. Our proposed CSPs provide a wide range of SaaS, PaaS, and IaaS offerings.	7
Table 3: Annual Growth and Team Retention Rates.	13
Table 4: Depth and Breadth of Proposed Offerings. Amazon Web Services, Microsoft, VMware, and SoftLayer offer a broad set of IaaS, PaaS, and SaaS offerings.	16
Table 5: Gartner and Forrester Research. Amazon Web Services, Microsoft, VMware, and SoftLayer are the clear leaders and principles in the IaaS and PaaS market.	17
Table 6: CSA STAR Auditing Capabilities and Reports. Emergent's proposed CSPs possess auditing capabilities and produce reports consistent with SAS 70 or later versions, including SSAE 16 6/2011 or greater.	19
Table 7: Billing and Pricing Practices. AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each offer multiple ways to purchase their services.	20
Table 8: NIST Cloud Computing Service and Deployment Models. Emergent's proposed cloud solutions meet the requirements of NIST SP 800-145.	21
Table 9: Amazon Web Services is the agile and innovative market leader. AWS has more cloud IaaS compute capacity in use than the aggregate total of ALL other Cloud Service Providers combined.	22
Table 10: Microsoft Azure unifies IaaS and PaaS components. Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web—for moving faster, achieving more, and saving money.	23
Table 11: VMware vCloud Air. A secure public cloud service operated by VMware, built on the trusted foundation of VMware vSphere.	25
Table 12: SoftLayer. Developed the industry's first Network-Within-a-Network topology for true out-of-band access and offers an easy-to-use customer portal and robust API for full remote-access of all product and service management options.	27
Table 13: AWS Best Practices. Built-in Security Features.	29
Table 14: AWS Best Practices. Visibility into Data, Performance, and Resource Usage.	30
Table 15: Microsoft Best Practices. Security Design and Operations.	32
Table 16: Microsoft Best Practices. Visibility, Compliance, Data Security and Threat Protection.	32
Table 17: VMware Best Practices. Cloud Computing Security.	34
Table 18: VMware Best Practices. Visibility, Compliance, Data Security and Threat Protection.	34
Table 19: SoftLayer Best Practices. Multi-Layer Security Strategy.	35
Table 20: SoftLayer Best Practices. Visibility, Compliance, Data Security and Threat Protection.	36
Table 21: FedRAMP Requirement, Standards, and Guidance. One of the benefits of receiving FedRAMP Authorization is significant savings in terms of cost, time, and resources—"do once, use many times".	42
Table 22: NIST Essential Characteristics of Cloud Computing. Emergent's proposed SaaS, PaaS, and IaaS offerings all meet the guidelines of NIST SP 800-145.	43
Table 23: Service Model Subcategories. Our proposed CSPs provide a wide range of SaaS, PaaS, and IaaS offerings.	47
Table 24: Incident Response Procedures. A host of factors contribute to the lack of detail provided in the public domain.	51
Table 25: A.13 Information Security Incident Management. Reporting and managing security events, weaknesses, and improvements.	52
Table 26: A.14 Business Continuity Management. Mitigating the risk of major failures and planning for timely resumption.	53
Table 27: A.15 Compliance. Conforming to legal requirements, organizational security policies and standards and minimizing the performance impact of implementing audit controls.	53
Table 28: NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology.	55
Table 29: AWS Support Plans. Customers receive basic support at no cost and have the option to increase the level of support.	58
Table 30: AWS Support. Response times vary based on the level of support and the severity of the request.	59

Table 31: Microsoft Azure Support. <i>All levels of support are paid-for services and have the option to increase the level of support.</i>	59
Table 32: VMware vCloud Support. <i>All levels of support are paid-for services and have the option to increase the level of support.</i>	60
Table 33: SoftLayer Support. <i>Support is provided at no additional cost.</i>	61
Table 34: Cloud Compliance and Security. <i>Our CSPs conform to global industry standards—verified by third-party audits.</i>	65
Table 35: Securing Data and Applications from Threats. <i>AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each have different approaches to securing data and applications from threats inside and outside their service centers.</i>	66
Table 36: Ensuring Data Confidentiality. <i>AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer have data confidentiality standards and practices restricting access to customer data.</i>	68
Table 37: sdds.	70
Table 38: Encryption Technologies and Options. <i>AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer offer different encryption technologies and options to protect sensitive data while in or at rest.</i>	76
Table 39: Performance Measures and Reporting. <i>While each of our proposed CSPs guarantees different levels of “uptime”, they all exceed 99.9%.</i>	79
Table 40: Performance Measures and Reporting. <i>Each of our propose CSPs offer views with respect to their service performance and status.</i>	81
Table 41: Multiple Data Center Support. <i>AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each support multiple data centers located within the United States.</i>	83
Table 42: Identity and Access Management. <i>AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each have different approaches to providing IAM capabilities.</i>	84
Table 43: Antivirus and Antimalware. <i>AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each have different approaches to providing protection from viruses and malware.</i>	86
Table 44: Integration and Customization. <i>Both open and proprietary solutions from our proposed CSPs can be customized and integrated to existing environments.</i>	90

Section Title: RFP Signature Page

The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of the RFP.

Requirement 5.1 (M) SIGNATURE PAGE

Proposals must be submitted with a vendor information form, located on Bidsync as an attachment to the RFP, which must contain an ORIGINAL HANDWRITTEN signature executed in INK OR AN ELECTRONIC SIGNATURE, and be returned with the Offeror's proposal.

Emergent has submitted signed RFP Signature Page and Vendor Information forms as addenda to this proposal:

- ✓ 1 Emergent RFP Signature Page CH16012.pdf
- ✓ 2 Emergent Vendor Information Form CH16012.pdf

Section Title: Executive Summary

By selecting Emergent, NASPO/Value Point will have a partner dedicated its customers. Our approach is simple: to identify the customer's cloud computing needs and provide the service that best meets those needs. We are proposing 4 of the top cloud services providers in the world.

Substantiation

The voice of well-respected and independent 3rd parties is generally the best way to substantiate claims. Gartner and Forrester have recently summarize the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) marketplace and provided commentary on various IaaS and PaaS offerings in the following reports:

- ✓ [Gartner Magic Quadrant for Cloud Infrastructure as a Service, 18 May 2015ⁱ](#)
- ✓ [Gartner Magic Quadrant for Enterprise Application Platform as a Service, 24 March 2015ⁱⁱ](#)
- ✓ [The Forrester Wave™: Enterprise Public Cloud Platforms, Q4 2014ⁱⁱⁱ](#)

Depth and Breadth of Proposed Solutions

Amazon Web Services Initially a provider of IaaS, AWS offers a broad set of global compute, storage, database, analytics, application, and deployment services that help customers move faster, lower IT costs, and scale applications. These services are trusted by the largest enterprises and the hottest start-ups to power a wide variety of workloads including: web and mobile applications, IoT, game development, data processing and warehousing, storage, archive, and many others.

- ✓ AWS offers IaaS, PaaS, and SaaS (both natively and through their AWS Partner Network (APN))

Microsoft Azure Initially a provider of PaaS, Azure offers a range of cloud services, including those for compute, analytics, storage and networking. Customer can pick and choose from these services to quickly build, deploy, and manage new and existing applications across a global network of Microsoft-managed datacenters:

- ✓ Microsoft Azure offers IaaS, PaaS, and SaaS (both natively and through their Microsoft Azure Marketplace)

VMware vCloud Air vCloud Air is a collection of cloud services built on VMware's vSphere. Although proprietary, VMware has a huge presence in the public sector.

- ✓ VMware has a wide range of PaaS and SaaS offerings available from the vCloud Air Solution Exchange.

SoftLayer SoftLayer offers one of the highest performing cloud infrastructures available—one platform that takes data centers around the world that are full of the widest range of cloud computing options, and then integrates and automates everything.

- ✓ Though most closely representing a “pure-play” IaaS offering, SoftLayer has a wide range of PaaS and SaaS offerings available from its Technology Partners Marketplace.

Information Provided

Emergent is providing website links and/or URLs in its response due to the overwhelming volume of documents we are providing, since we are a reseller and our offering is comprised of services supplied by several different manufacturers. As a result, such website links and/or URLs may be necessary and reasonable to clarify certain, applicable manufacturer terms and conditions. In addition, such links and/or URLs are being provided for current informational purposes only and Emergent bears no responsibility for the accuracy, legality or content of the information, which is in the control of and subject to change by the applicable manufacturers as terms and conditions will evolve over time in accordance with updates to the manufacturer offerings.

Section Title: Mandatory Minimums

This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.

If applicable to an Offeror's offering, an Offeror must provide a point by point responses to each mandatory minimum requirement. If a mandatory minimum requirement is not applicable to an Offeror's offering then the Offeror must explain why the mandatory minimum requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

Requirement 5.2 (M) COVER LETTER

Proposals must include a cover letter on official letterhead of the Offeror. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed. In addition, the cover letter must include:

Emergent has submitted its Cover Letter as addenda to this proposal:

✓ 3 Emergent Cover Letter CH16012 (signed).pdf

16 August 2016

Christopher Hughes, Assistant Director
State of Utah, Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Subject: NASPO ValuePoint and the State of Utah Request for Proposal CH16012 Cloud Solutions

Mr. Hughes,

Emergent is pleased to present to you a proposal that will demonstrate that Emergent is fully qualified and available to provide the cloud solutions required for this contract to be successful and the best value for NASPO/ValuePoint.

As requested in the RFP document, Mythics attests to the following:

Requirement 5.2.1

A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

Emergent understands that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

Requirement 5.2.2

A statement naming the firms and/or staff responsible for writing the proposal.

The following Emergent staff was responsible for writing this proposal:

- James Flint
- Lynn Brogis
- Venkat Sundaram

Emergent also received content from Amazon Web Services and SoftLayer.

Requirement 5.2.3

A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

Emergent is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

Requirement 5.2.4

A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

Emergent acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

Requirement 5.2.5

A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.

Emergent is capable of providing the following cloud offerings under the terms of the RFP.

Table 1: NIST Cloud Computing Service and Deployment Models. *Emergent's proposed cloud solutions meet the requirements of NIST SP 800-145.*

Cloud Service Provider	Service Model(s)	Deployment Model(s)	Risk Category
Amazon Web Services	IaaS, PaaS, SaaS	Private, Public, Hybrid	Moderate/Low
Microsoft Azure	IaaS, PaaS, SaaS	Private, Public, Hybrid	Moderate/Low
VMware vCloud Air	IaaS, PaaS, SaaS	Public, Hybrid	Moderate/Low
SoftLayer	IaaS	Private, Public, Hybrid	Moderate/Low

All of our proposed CSPs offer SaaS, PaaS, and IaaS having received either Joint Authorization Board (JAB) Provisional Authorization or an Agency FedRAMP Authorization. In the spirit of the “do once, use many times”, for each proposed offering, Emergent has identified the applicable NIST Cloud Computing Service and Deployment Models as approved by FedRAMP.

NOTE: FedRAMP Authorization is not necessarily applicable to other solutions found in each CSP’s respective Marketplace.

Table 2: Service Model Subcategories. *Our proposed CSPs provide a wide range of SaaS, PaaS, and IaaS offerings.*

Service Model/Subcategory	Amazon Web Services	Microsoft Azure	VMware vCloud Air	SoftLayer
IaaS: Computer/Infrastructure Services/Operating systems	Yes	Yes	Yes	Yes
IaaS: Computer/Infrastructure Services/Hypervisors	Yes	Yes	Yes	Yes
IaaS: Disaster Recovery/Business Continuity	Yes	Yes	Yes	Yes

IaaS: Disaster Recovery/High Availability / Failover	Yes	Yes	Yes	Yes
IaaS: GIS	Yes	Yes	Marketplace	Marketplace
IaaS: Storage/File	Yes	Yes	Yes	Yes
IaaS: Storage/Block	Yes	Yes	Yes	Yes
IaaS: Storage/Object	Yes	Yes	Yes	Yes
IaaS: Storage/Archive	Yes	Yes	Yes	Yes
IaaS: Storage/Cache	Yes	Yes	Yes	Yes
IaaS: Storage/Content Delivery Networks (CDN)	Yes	Yes	Yes	Yes
IaaS: Storage/Litigation Hold	Yes	Yes	Yes	Marketplace
IaaS: Network/Virtual network	Yes	Yes	Yes	Yes
IaaS: Network/Load balancer	Yes	Yes	Yes	Yes
IaaS: Network/DNS	Yes	Yes	Yes	Yes
IaaS: Network/Gateway (e.g. VPN or Application)	Yes	Yes	Yes	Yes
IaaS: Network/Firewall	Yes	Yes	Yes	Yes
IaaS: Network/Traffic manager	Yes	Yes	Yes	Yes
IaaS: Network/Direct link	Yes	Yes	Yes	Yes
IaaS: PC/Desktop "aaS"	Yes	Yes	Yes	Marketplace
IaaS: Security/Identity & Access Management	Yes	Yes	Yes	Yes
IaaS: Security/Encryption	Yes	Yes	Yes	Yes
IaaS: Security/Data Loss Prevention (DLP)	Yes	Yes	Yes	Yes
IaaS: Security/Web Security	Yes	Yes	Yes	Yes
IaaS: Security/Email Security	Yes	Yes	Yes	Yes
IaaS: Security/Network Security	Yes	Yes	Yes	Yes
IaaS: Security/Security Information and Event Management (SIEM)	Yes	Yes	Yes	Yes
IaaS: Security/Intrusion Management	Yes	Yes	Yes	Yes
IaaS: Security/DDOS Monitoring / Management	Yes	Yes	Yes	Yes
IaaS: Other (identify additional sub-categories and/or descriptors)	Yes	Yes	Yes	Yes
PaaS: Analytics/Hadoop	Yes	Yes	Yes	Yes
PaaS: Analytics/Business Intelligence	Yes	Yes	Marketplace	Marketplace
PaaS: Analytics/Data Warehouse	Yes	Yes	Yes	Yes
PaaS: Database/Relational	Yes	Yes	Yes	Yes
PaaS: Database/NoSQL	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Containers	Yes	Marketplace	Yes	Yes
PaaS: Development, Testing and Deployment/Services and APIs	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Mobile	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Internet of Things	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Tools	Yes	Yes	Yes	Yes

PaaS: Development, Testing and Deployment/Runtime environments	Yes	Yes	Yes	Yes
PaaS: Electronic Records Management	Marketplace	Marketplace	Marketplace	Yes
PaaS: E-Discovery	Marketplace	Marketplace	Marketplace	Yes
PaaS: GIS	Marketplace	Marketplace	Marketplace	Yes
PaaS: Integration (iPaaS)	Yes	Yes	Yes	Yes
PaaS: Open Source	Yes	Yes	Yes	Yes
PaaS: Other (identify additional sub-categories and/or descriptors)	Gaming, Mobile, Desktop	Marketplace	Marketplace	Yes
SaaS: Data Analytics	Yes	Yes	Marketplace	Yes
SaaS: Business Intelligence	Yes	Yes	Marketplace	Yes
SaaS: Business Continuity/Disaster Recovery	Yes	Yes	Marketplace	Yes
SaaS: Cloud and Infrastructure Management Tools	Yes	Yes	Marketplace	Yes
SaaS: Collaboration	Marketplace	Yes	Marketplace	Yes
SaaS: Customer Relationship Management	Marketplace	Yes	Marketplace	Yes
SaaS: Citizen Relationship Management	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Data Management	Yes	Yes	Marketplace	Yes
SaaS: E-Discovery	Marketplace	Marketplace	Marketplace	Yes
SaaS: Electronic Records Management	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace
SaaS: ERP/HR	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Finance	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Budget	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Procurement	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace
SaaS: GIS	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Human Resource/Payroll	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Human Resource/Time, Attendance and Scheduling	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Human Resource/Recruitment and Hiring	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Internet Filtering	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Licensing and Registration Systems	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Office Productivity/Word Processing	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Document Tracking	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/E-mail	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Spread sheets	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Presentation	Yes	Yes	Marketplace	Yes
SaaS: Message Filtering	Yes	Yes	Marketplace	Yes
SaaS: Meeting Planning, hosting, conferencing	Marketplace	Yes	Marketplace	Yes

SaaS: Mobile Data Management	Marketplace	Yes	Marketplace	Yes
SaaS: Point of Sale (POS)	Yes	Yes	Marketplace	No
SaaS: Procurement Systems	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Project and Portfolio Management (PPM) Tools.	Marketplace	Yes	Marketplace	Yes
SaaS: Security	Yes	Yes	Yes	Yes
SaaS: Travel Management	Marketplace	Yes	Marketplace	Marketplace
SaaS: Workflow and Electronic Signature	Marketplace	Yes	Marketplace	Marketplace
SaaS: Other (identify additional sub-categories and/or descriptors)	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace

Requirement 5.2.6

A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.

- ✓ Please see Emergent's response to Requirement 5.2.5, specifically **Table 1** identifying the data risk categories that our proposed CSPs are capable of storing.

Respectfully,

Paul Kohler
Executive Vice President
Emergent, LLC

Requirement 5.3 (M) ACKNOWLEDGEMENT OF AMENDMENTS

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.

Emergent has submitted a signed Acknowledgement form as addenda to this proposal:

✓ 4 Emergent AoA CH16012.pdf

Requirement 5.5 (M) GENERAL REQUIREMENTS

Requirement 5.5.1

Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

Emergent agrees agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

Requirement 5.5.2

Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

Emergent agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

Requirement 5.5.3

Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or to submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both documents.

Emergent has submitted a Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Self-Assessment from each CSP as addenda to this proposal:

Amazon Web Services ✓ 5 AWS_Risk_and_Compliance_Whitepaper.pdf (pages 25-61)

Microsoft Azure ✓ 6 Microsoft-Azure-CCM-v3.0.1-11-09-2015.docx

VMware vCloud Air ✓ 7 VMware-vCloud-Air-CAIQ-v1.0-2014-12-30.pdf

SoftLayer ✓ 8 Softlayer-CAIQ-v3.0.1-2016-01-08.xls

Each document may be found on the [CSA](#) website.

Requirement 5.5.4

Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Applicable and up-to-date Service Level Agreements (SLAs) can be found on the websites of each of our proposed CSPs:

Amazon Web Services	<u>Amazon CloudFront Service Level Agreement</u> <u>Amazon EC2 Service Level Agreement</u> <u>Amazon RDS Service Level Agreement</u> <u>Amazon Route 53 Service Level Agreement</u> <u>Amazon S3 Service Level Agreement</u>
Microsoft Azure	<u>Individual Azure Service Level Agreements</u>
VMware vCloud Air	<u>vCloud Air Service Level Agreement</u>
SoftLayer	<u>SoftLayer Service Level Agreement</u>

Requirement 5.7 RECERTIFICATION OF MANDATORY MINIMUMS AND TECHNICAL SPECIFICATIONS

Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.

If awarded a contract under the RFP, Emergent is willing to annually meet with the Lead State to determine whether or not the services offered meet or exceed the technical capabilities stated in Emergent's response to the Solicitation, since the manufacturers' services will evolve over time and Emergent cannot control the manner in which they will evolve.

Section Title: Business Profile

Founded independently in 2006 and subsequently folded into Mythics, Inc. as a wholly owned subsidiary, Emergent, LLC is an award-winning Value Added Reseller and GSA Schedule Holder focused on solving complex business and mission challenges on behalf of Government, Commercial, Education and Healthcare sectors through the creative use of IT.

Emergent provides custom managed services offerings, along with end-to-end guidance and support in a full range of disciplines:

- **Security.** Information security is integral to the success of any organization. It protects the confidentiality, integrity, and availability of systems and data. It prevents the release and the modification of sensitive information to unauthorized individuals and provides accessibility to data at all times. Emergent offers security solutions from Symantec, FireEye and more...
- **Open Source.** Open source technologies are secure, high quality, affordable solution options to help tackle a wide range of IT challenges. Emergent offers a comprehensive portfolio of open source solutions from Red Hat, Alfresco and more...
- **Cloud Computing.** Cloud computing offers a flexible new approach to delivering your IT services, one that can respond quickly to your business and agency's needs. Emergent can help you transition to this new approach transforming your current IT environment to support more flexible, agile, service delivery with improved security and control. Emergent represents industry leading cloud-computing solutions through partnerships with AWS, Microsoft, VMware, SoftLayer, Google, EMC and more...
- **Collaboration and Desktop Applications.** Emergent provides a deep portfolio of complementary applications for telework and collaboration, web publishing, training, technical communication, enterprise resource planning (ERP), customer relationship management (CRM) and financial/ human resource management. Emergent represents the full product suites from Adobe, ConnectSolutions, Citrix and more...
- **Networking.** Networking solutions enable you to virtualize and manage vital information, while delivering unique capabilities for a more flexible IT infrastructure. Emergent offers an extensive portfolio of networking solutions and services from manufacturers such as Cisco, Dell, HP and more...

Table 3: Annual Growth and Team Retention Rates.

Corporate Annual Growth					State and Local Team Retention		
Year	Starting Headcount	Ending Headcount	Increase	Growth Rate	Starting Team Size	Individuals Employed throughout duration of Measurement Period	Retention Rate
2015	263	278	15	5.70%	18	17	94.50%
2014	224	263	39	17.40%	15	14	93.30%
2013	203	224	21	10.30%	13	13	100%

Requirement 6.2 (M)(E) SCOPE OF EXPERIENCE

Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the business provided offerings identical or very similar to those required by this RFP. Government experience is preferred.

Contract	Total Revenue
GSA Schedule 70	\$31,847,676
NASA SEWP V (Category D)	\$20,920,094
NIH ECS III	\$13,349,041
NASA SEWP V (Category A)	\$12,372,363
BPA: US Courts	\$7,550,650
NIH CIO-CS	\$2,580,403.88

Requirement 6.3 (M) FINANCIALS

Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

Emergent, LLC is a wholly owned subsidiary of Mythics, Inc. In the past, we have experienced issues with confidentiality matters; therefore, we are providing the following information. If the State should have any further questions, please contact the undersigned.

Mythics D&B Number: 013358002

Mythics Credit Rating: 1R3

Gross Revenue 2014: \$937,688,000 (calendar year)

Gross Revenue 2013: \$798,907,000 (calendar year)

Emergent has submitted a copy of its authorization to resell services from each of our proposed CSPs as addenda to this proposal

✓ 9 Emergent Auditor Statement CH16012.pdf

Requirement 6.4 (E) GENERAL INFORMATION

Requirement 6.4.1

Provide any pertinent general information about the depth and breadth of your Solutions and their overall use and acceptance in the cloud marketplace.

The following sections include excerpts from the aforementioned Gartner and Forrester reports.

Amazon Web Services	AWS offers virtualized multitenant and single-tenant compute, with multitenant storage, along with extensive additional IaaS and PaaS capabilities, including object storage with an integrated CDN (Amazon S3 and CloudFront) and a Docker container service (EC2 Container Service). It is willing to negotiate large-scale single-tenant and on-premises deals (such as the U.S. intelligence community cloud deal). The AWS Marketplace has an extensive selection of third-party software and services. Enterprise-grade support is extra. It has a multi-fault-domain SLA. Colocation needs are met via AWS Direct Connect. ⁱ
Microsoft Azure	Microsoft Azure offers Hyper-V-virtualized multitenant compute (Virtual Machines), with multitenant storage, along with many additional IaaS and PaaS capabilities, including object storage (Blob Storage) and a CDN. The Azure Marketplace offers third-party software and services. Enterprise-grade support is extra. It has a multi-fault-domain SLA. Colocation needs are met via Azure ExpressRoute. See the In-Depth Assessment for a detailed technical evaluation. ⁱ
VMware vCloud Air	vCloud Air is a VMware-virtualized, vCloud-API-enabled offering that comes in three variants: On-Demand (fully multitenant), Virtual Private Cloud (fully multitenant and SRP-priced) and Dedicated Cloud (single-tenant compute with multitenant back-end, and SRP-priced with customer-controlled oversubscription). There is also a disaster recovery service. All vCloud Air services share a common portal and are delivered as resource pools out of the same shared hardware. ⁱ
SoftLayer	SoftLayer, an IBM company, offers both multitenant and single-tenant Citrix-Xen-virtualized compute (Virtual Servers). It also offers, as part of its cloud, paid-by-the-hour non-virtualized dedicated servers (Bare Metal Servers). It has OpenStack-based object storage with an integrated CDN (via a partnership with EdgeCast). SoftLayer's primary business is non-cloud offerings, such as paid-by-the-month dedicated servers (a broader range of configurations than is available per hour) and hosted appliances. ⁱ

In addition, each CSP has broken from their roots and introduced Software as a Service (SaaS) offerings to augment their IaaS and PaaS portfolios, as described in **Table 4:** below.

Table 4: Depth and Breadth of Proposed Offerings. *Amazon Web Services, Microsoft, VMware, and SoftLayer offer a broad set of IaaS, PaaS, and SaaS offerings.*

CSP	Depth and Breadth of Offering
Amazon Web Services	Initially a provider of IaaS, AWS offers a broad set of global compute, storage, database, analytics, application, and deployment services that help customers move faster, lower IT costs, and scale applications. These services are trusted by the largest enterprises and the hottest start-ups to power a wide variety of workloads including: web and mobile applications, IoT, game development, data processing and warehousing, storage, archive, and many others. • IaaS. Compute, Database, Storage & Content Delivery, and Networking • PaaS. Analytics, Enterprise Applications, Mobile Services, and Internet of Things • SaaS. Productivity/Operational Efficiency. Developer Tools, Application Services, Management Tools, and Security & Identity AWS also has thousands of organizations in the AWS Partner Network (APN) including system integrators, consulting firms, and independent software vendors (ISVs) offering SaaS: • Technology Partners. The AWS Partner Network is made up of a strong and growing community of companies that offer a wide range of products and services on the AWS platform. • AWS Marketplace. An online software store with over 2,300 listings to buy and immediately start using SaaS that runs on AWS.
Microsoft Azure	Initially a provider of PaaS, Azure offers a range of cloud services, including those for compute, analytics, storage and networking. Customer can pick and choose from these services to quickly build, deploy, and manage new and existing applications across a global network of Microsoft-managed datacenters: • IaaS. Compute, Storage, Networking, Identity and Access Management, Media and CDN • PaaS. Web & Mobile, Database, Analytics, Management and Security, Internet of Things, Hybrid Integration • SaaS. Productivity/Operational Efficiency. Developer Services Azure has a wide range of PaaS and SaaS offerings available from the Microsoft Azure Marketplace.
VMware vCloud Air	vCloud Air is a collection of cloud services built on VMware's vSphere. IaaS: • Dedicated Cloud. Dedicated physical infrastructure compute service sold as a subscription. • Virtual Private Cloud. Logically isolated, multi-tenant compute service sold as a subscription. • Virtual Private Cloud OnDemand. Logically isolated, multi-tenant compute service that does not require a resource commitment or long-term contract. • Object Storage. A scalable and resilient storage solution for unstructured data. Offers customers self-service access to storage capacity on-demand and enables them to scale up to petabytes from any web environment. PaaS: • Disaster Recovery. Marketed as a "Recovery-as-a-Service" offering, it provides simple, affordable protection in the cloud for a customer's vSphere environment. Software as a Service: • Horizon Air. A managed service offering to securely deploy desktops and applications rapidly as an easily managed, integrated cloud service. End users access their desktops and apps securely from any device or browser • vRealize Air. A SaaS suite that enables customers to deliver and manage infrastructure services for private and public clouds, hypervisors and physical infrastructure. • vCloud Air Hybrid Cloud Manager. A feature-rich management SaaS solution for extending vSphere workloads into vCloud Air. Each service offers a variety of features and a selection of Add-Ons to meet customer needs:

	• Data Protection • Direct Connect • Advanced Networking Services • Hybrid Cloud Manager • Offline Data Transfer <i>VMware has a wide range of PaaS and SaaS offerings available from the vCloud Air Solution Exchange.</i>
SoftLayer	SoftLayer offers one of the highest performing cloud infrastructures available—one platform that takes data centers around the world that are full of the widest range of cloud computing options, and then integrates and automates everything. • Cloud Servers • Cloud Storage • Networking • Security • Developers • Management Controls and Tools <i>SoftLayer has a wide range of PaaS and SaaS offerings available from its Technology Partners Marketplace.</i>

Use and Acceptance of Solutions in the Marketplace

Gartner and Forrester are two of the most influential information technology research and advisory companies in the world. In their most recent analysis of the IaaS and PaaS platforms, both firms came to similar conclusions about the market, that *Amazon Web Services, Microsoft Azure, VMware vCloud Air, and SoftLayer are the clear leaders and principle visionaries in the IaaS and PaaS market.*

Table 5: Gartner and Forrester Research. Amazon Web Services, Microsoft, VMware, and SoftLayer are the clear leaders and principles in the IaaS and PaaS market.

CSP	Excerpts from Gartner and Forrester Reports
Amazon Web Services	✓ “cloud-focused service provider with a very pure vision of highly automated, cost-effective IT capabilities, delivered in a flexible, on-demand manner”ⁱ ✓ “Recommended uses: All use cases that run well in a virtualized environment”ⁱ ✓ “the broadest range of use cases...is the overwhelming market share leader...extensive network of partners”ⁱ ✓ “a thought leader; it is extraordinarily innovative, exceptionally agile, and very responsive to the market...richest array of IaaS features and PaaS-like capabilities...the provider most commonly chosen for strategic adoption”ⁱ ✓ “best fit for the DevOps pro segment...the capabilities of AWS’ application services, coupled with its mature infrastructure services, vast ecosystem of partners...gave it high current offering and strategy scores...also excels in breadth of security, reliability, and compliance characteristics”ⁱⁱⁱ ✓ “leads in maturity and breadth”ⁱⁱⁱ
Microsoft Azure	✓ “Recommended uses: General business applications and development environments for Microsoft-centric organizations; cloud-native applications; batch computing”ⁱ ✓ “integrated IaaS and PaaS components that operate and feel like a unified whole...rapidly rolling out new features and services, including differentiated capabilities...services seamlessly extend and interoperate with on-premises Microsoft infrastructure”ⁱ ✓ “growing rapidly, and is in second place for market share, with more than twice as much cloud IaaS compute capacity in use as the aggregate total of the remaining providers in this Magic Quadrant (excluding market share leader AWS)”ⁱ ✓ “Windows developers familiar with .NET languages and frameworks find Azure a natural environment

	from which to move to cloud application development” ⁱⁱ ✓ “Microsoft’s Azure is the best fit for coders, but a good choice for DevOps. Azure is maturing rapidly...simplified the developer experience and added application and infrastructure services that appeal to coders and DevOps pros” ⁱⁱⁱ ✓ “Azure is a full service platform with solid infrastructure services, robust application services, a solid partner ecosystem, and strong integrations with its tools...” ⁱⁱⁱ
VMware vCloud Air	✓ “Recommended uses: Development environments, general business applications, supplementing existing VMware-virtualized environments” ⁱ ✓ “market share leader and thought leader in virtualization...strong brand, global sales reach, and a broad base of existing customers that are deeply committed to its technologies” ⁱⁱ
SoftLayer	✓ “Recommended uses: E-business hosting, general business applications and batch computing... control over scalable infrastructure and bare-metal servers in order to meet requirements for performance, regulatory compliance or software licensing” ⁱ ✓ “IBM’s portfolio...has IaaS, PaaS and SaaS elements, along with IT operations management (ITOM) software, middleware and database software, and comprehensive consulting and outsourcing capabilities...SoftLayer will be the common hosting platform for IBM’s services in the future” ⁱ ✓ “IBM has a strong brand and existing customer relationships across the globe...intends to make local presence one of its competitive differentiators” ⁱ ✓ “IBM’s public cloud platform now comprises SoftLayer for infrastructure services...SoftLayer allowed IBM to rapidly expand its global public-cloud footprint...is now bringing its many middleware and SaaS properties to SoftLayer” ⁱⁱⁱ ✓ “With SoftLayer, IBM has a solid infrastructure platform...services are mature and expanding with new data centers around the world” ⁱⁱⁱ

Requirement 6.4.2

Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

Because the Statement on Auditing Standards No. 70 (SAS 70) standard was improperly used to assess Cloud Service Provider controls, the American Institute of Certified Public Accountants (AICPA) developed the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) for service auditors.

Like the SAS 70 standard, the SSAE 16 standard provides guidance to auditors assessing controls at a service organization relevant to user entities internal control over financial reporting. SSAE 16 requires a service organization to describe its system and define its control objectives and controls relevant to its internal control over financial reporting along with a written assertion by management. Two (2) types of SSAE 16 reports are to be issued, a Service Organization Control (SOC) 1, Type 1 and a SOC 1, Type 2.

Two additional reports, the SOC 2 and SOC 3, are based on AT Section 101, Attest Engagements. Although SOC 2 and SOC 3 reports differ in content and purpose, both use the AICPA’s Trust Services Principles (TSP) and criteria specifically defined for security, availability, confidentiality, processing integrity, and privacy. A SOC 2 report is largely a restricted-use report, containing a detailed description of the service auditor's tests of controls and results of those tests as well as the service auditor's opinion on the description of the service organization's system. A SOC 3 report is a generally a public facing report providing only the auditor's report on whether the system achieved the trust services criteria.

Table 6: CSA STAR Auditing Capabilities and Reports. Emergent's proposed CSPs possess auditing capabilities and produce reports consistent with SAS 70 or later versions, including SSAE 16 6/2011 or greater.

CSP	Level of Disclosure with CSA STAR
Amazon Web Services	AWS releases semi-annual SOC 1, SOC 2, and SOC 3 reports in mid-May and mid-November. - Publicly available AWS SOC 1 Control Objectives (page 19) - Publicly available SOC 3 Report - SOC 1 and SOC 2 reports available to customers upon request
Microsoft Azure	Azure is audited annually for both SOC 1 Type 2 and SOC 2 Type 2. - Publicly available Compliance Framework for Online Services - Publicly available SOC 3 Report - SOC 1 and SOC 2 reports is restricted to customers who have signed nondisclosure agreements with Microsoft
VMware vCloud Air	vCloud Air is audited annually for both SOC 1 Type 2 and SOC 2 Type 2. - Publicly available vCloud Air SOC1 Matrix - Publicly available SOC 3 Report - Copy of the SOC 2 Type 2 is available upon request
SoftLayer	SoftLayer is audited annually for both SOC 1 Type 2 and SOC 2 Type 2. - Publicly available SOC 3 Report - Copy of the SOC 2 Type 2 is available to customers via the portal and upon request for non-customers

6.5 (E) BILLING AND PRICING PRACTICES

Requirement 6.5.1 and 6.5.2

Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.

Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.

While each of our proposed CSPs offers multiple ways to purchase their services, described in **Table 7** below, they all have one thing in common: the more a customer commits to up front, the greater the savings. But by doing so, customers distance themselves from the basic tenets of cloud computing. As it is with all things cloud, it is up to the responsibility of the customer to properly analyze the costs impacts.

Table 7: Billing and Pricing Practices. AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each offer multiple ways to purchase their services.

CSP	Billing and Pricing Practices
Amazon Web Services	Pay-as-You-Go. No minimum commitment or long-term contract is required. Customers can turn off cloud resources and stop paying for them when they are not needed, maximizing Return on Investment (ROI) through full utilization. Pay-Less-When-You-Reserve. For certain AWS products, customers can invest in reserved capacity, paying a low up-front fee to receive a significant discount. This results in overall savings of up to 60% (depending on the type of instance reserved) over equivalent on-demand capacity. Pay Even Less Per Unit by Using More. AWS pricing is tiered for storage and data transfer, so the more customers use, the less they pay per gigabyte. Pay Even Less as AWS Grows. We continually focus on reducing our data center hardware costs, improving our operational efficiencies, lowering our power consumption, and passing savings back to customers. AWS has a history of continually lowering prices and has reduced prices 51 times since AWS launched in 2006. Transparency. AWS provides transparent, publicly available, and up-to-date pricing, and tools that allow customers to evaluate AWS pricing against other Cloud Service Providers (CSPs). AWS's Simple Monthly Calculator can be found at http://calculator.s3.amazonaws.com/index.html. Governance. AWS provides tools to generate detailed and customizable billing reports to meet customer business and compliance needs. Additionally, AWS Partner Network (APN) Consulting Partners can help customers manage and control cost utilization/tracking tools in order to provide customized billing reports.
Microsoft Azure	Pay-As-You-Go Subscriptions. The most popular and flexible payment plan because there are no minimum purchases or commitments and customers can cancel anytime. Customers can pay by credit card or by invoice. Prepaid Subscriptions. Microsoft's 12-month prepaid subscription for Azure services lets customer earn discounts on the amount they prepay. If customer service consumption exceeds the prepaid amount, they can make an additional prepayment to continue getting the discount, or simply pay as they go for future usage. Customers can pay by credit card or by invoice. Microsoft Resellers. Customers can work with the same resellers that they already purchase Microsoft software from using the Open Volume License Program. If customers have purchased Azure from a reseller and have an Open license key, customers can activate their Azure subscription. Enterprise Agreements. Large organizations often sign up for a Microsoft Enterprise Agreement (EA). By making an upfront usage commitment to Azure they earn several additional benefits—including flexible billing options and best prices. Microsoft Azure Compute Option. This lowers compute costs and mitigates budget risks associated with unplanned deployments, while retaining the flexibility of on-demand, hourly consumption Microsoft Azure Hybrid Use Benefit. Run Windows Server Virtual Machines on Azure at base compute pricing. Windows Server customers with Software Assurance are eligible for this benefit.
VMware vCloud Air	Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery are each offered in monthly and annual subscription terms. Subscription Services are sold with one increment of compute, support, storage, and bandwidth as well as a pre-defined number of Public IPs. Customers can select additional increments of the above resources as needed to accommodate their cloud environment. OnDemand pricing is based upon a standard rate per unit metric (e.g. GB/hr, vCPU/hr, GB/mo, IP/hr ,etc)
SoftLayer	SoftLayer offers clear, competitive pricing for high performance bare metal servers, virtual servers, and cloud services on hourly or monthly terms—and down to the server resource level to help customers gain control over infrastructure spend. Modular server pricing provides customers the ability to customize their cloud with only the resources they require. Rather than bundling services that customers may not need, SoftLayer lets customers choose the compute, RAM, storage, and network resources they want to provision and break down the price to show where the costs incur.

Total Cost of Ownership (TCO) Calculator

Each CSP provides a proprietary TCO calculator described below:

Amazon Web Services	The AWS TCO Calculator allows organizations to compare AWS to the cost of running applications in an on-premises or traditional hosting environment. The AWS Whitepaper The Total Cost of (Non) Ownership of Web Applications in the Cloud also helps customers understand the different cost factors involved in moving to AWS. Analysis shows that AWS offers significant cost savings (up to 80%) compared to equivalent on-premises deployments.
Microsoft Azure	Microsoft provides a pricing calculator to configure any combination of desired services (Compute, Web & Mobile, Data & Storage, Analytics, Internet of Things, Networking, Media and CDN, Hybrid Integration, Identity & Access Management, Developer Services, and Management & Security) to help customers estimate the costs.
VMware vCloud Air	The vCloud Air Pricing Calculators (OnDemand, Subscription, and Horizon Air) are available to help customers estimate the costs of using various vCloud Air services by configuring the desired combination of services and features.
SoftLayer	SoftLayer's TCO Calculator compare the cost of running applications in an on-premises or traditional hosting environment to SoftLayer. Customers can tailor an analysis to their situation with a comprehensive list of key TCO considerations.

Requirement 6.5.3

Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.

Emergent is capable of providing the following cloud offerings under the terms of the RFP.

Table 8: NIST Cloud Computing Service and Deployment Models. Emergent's proposed cloud solutions meet the requirements of NIST SP 800-145.

Cloud Service Provider	Service Model(s)	Deployment Model(s)	Risk Category
Amazon Web Services	IaaS, PaaS, SaaS	Public	Moderate
Microsoft Azure	IaaS, PaaS, SaaS	Public	Moderate
VMware vCloud Air	IaaS, PaaS, SaaS	Public, Hybrid	Moderate
SoftLayer	IaaS	Private, Public, Hybrid	Moderate

Emergent's proposed SaaS, PaaS, and IaaS offerings have all received either Joint Authorization Board (JAB) Provisional Authorization or an Agency FedRAMP Authorization. In the spirit of the "do once, use many times", for each proposed offering, Emergent has identified the applicable NIST Cloud Computing Service and Deployment Models as approved by FedRAMP.

The most current approved version of the requirements, standards, and guidance applicable to FedRAMP can be found in **Table 21**, below, and include NIST SP 800-145 *Definition of Cloud Computing* (NIST SP 800-145).

Additional information relating to this requirement:

- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
- ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Requirement 6.6 (E) SCOPE AND VARIETY OF CLOUD SOLUTIONS

Specify the scope and variety of the Solutions you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services and deployment models that you offer.

Scope and Variety: Amazon Web Services

AWS offers a broad set of global compute, storage, database, analytics, application, and deployment services that help customers move faster, lower IT costs, and scale applications. These services are trusted by the largest enterprises and the hottest start-ups to power a wide variety of workloads including: web and mobile applications, IoT, game development, data processing and warehousing, storage, archive, and many others.

Table 9: Amazon Web Services is the agile and innovative market leader. AWS has more cloud IaaS compute capacity in use than the aggregate total of ALL other Cloud Service Providers combined.

AWS Offering	Depth and Breadth	
IaaS	Compute - Virtual Servers - Containers 1-Click Web App Deployment - Event-Driven Compute Functions - Auto Scaling - Load Balancing Database - Relational - Database Migration - NoSQL - Caching - Data Warehouse	Storage & Content Delivery - Object Storage - CDN - Block Storage - File System Storage - Archive Storage - Data Transport - Integrated Storage Networking - Virtual Private Cloud - Direct Connections - Load Balancing - DNS
PaaS	Analytics - Business Intelligence - Data Warehouse - Machine Learning - Streaming Data	Mobile Services - Mobile Development - API Management - Identity - App Testing

	• Elasticsearch • Hadoop • Data Pipelines Enterprise Applications • Desktop Virtualization • Email & Calendaring • Document Sharing & Feedback	• Mobile Analytics • Development • Notifications Internet of Things • IoT Platform • Device SDK • Registry • Device Shadows • Rules Engine
SaaS and Productivity/Operational Efficiency	Developer Tools • Source Code Management • Code Deployment • Continuous Delivery Application Services • API Management • App Streaming • Search • Transcoding • Email • Notifications • Queueing • Workflow	Management Tools • Monitoring & Logs • Resource Templates • Usage & Resource Auditing • Dev/Ops Resource Management • Service Catalog • Performance Optimization Security & Identity • Access Control • SSL/TLS Certificates • Key Storage & Management • Identity Management • Security Assessment • Web Application Firewall

Scope and Variety: Microsoft Azure

Azure is a public cloud computing platform that provides a range of cloud services, including those for compute, analytics, storage and networking. Customer can pick and choose from these services to quickly build, deploy, and manage new and existing applications across a global network of Microsoft-managed datacenters.

Table 10: Microsoft Azure unifies IaaS and PaaS components. *Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web—for moving faster, achieving more, and saving money.*

Microsoft Azure Service	Depth and Breadth
Compute	• Virtual Machines. Provision Windows and Linux Virtual Machines in minutes • Cloud Services. Create highly available, infinitely scalable cloud applications and APIs • Batch. Run large-scale parallel and batch compute jobs • RemoteApp. Deploy Windows client apps in the cloud, run on any device • Service Fabric. Build and operate always-on, scalable, distributed applications • Azure Container Service. Use open source tools to deploy and manage containers
Web & Mobile	• App Service. Create web and mobile apps for any platform and any device • Web Apps. Quickly create and deploy mission critical Web apps that scale • Mobile Apps. Build and host the backend for any mobile app • Logic Apps. Automate the access and use of data across clouds without writing code • API Apps. Easily build and consume Cloud APIs • API Management. Publish APIs to developers, partners and employees securely and at scale

	- Notification Hubs. Scalable, cross-platform push notification infrastructure - Mobile Engagement. Maximize app usage, retention and monetization
Data & Storage	- SQL Database. Managed relational SQL Database-as-a-service - DocumentDB. Managed NoSQL document database-as-a-service - Redis Cache. High throughput, low latency data access to build fast and scalable applications - Storage: Blobs, Tables, Queues, Files and Disks. Durable, highly available and massively scalable cloud storage - StorSimple. Hybrid cloud storage for enterprises, reduces costs and improves data security - Search. Fully-managed search-as-a-service - SQL Data Warehouse. Elastic data warehouse-as-a-service with enterprise-class features - SQL Server Stretch Database. Dynamically stretch SQL Server databases to Azure
Analytics	- Data Lake Analytics. Distributed analytics service that makes big data easy - Data Lake Store. Hyperscale repository for big data analytics workloads - HDInsight. Provision managed Hadoop clusters - Machine Learning. Powerful cloud-based predictive analytics - Stream Analytics. Real-time stream processing - Data Factory. Orchestrate and manage data transformation and movement - SQL Data Warehouse. Elastic data warehouse-as-a-service with enterprise-class features - Data Catalog. Data source discovery to get more value from existing enterprise data assets
Internet of Things	- IoT Suite. Capture and analyze untapped data to improve business results - Azure IoT Hub. Connect, monitor, and control millions of IoT assets - Event Hubs. Receive telemetry from millions of devices - Stream Analytics. Real-time data stream processing from millions of IoT devices - Machine Learning. Powerful cloud based predictive analytics tool to enable predictive maintenance - Notification Hubs. A scalable, push notification engine for quickly sending millions of messages
Networking	- Virtual Network. Provision private networks, optionally connect to on-premises datacenters - ExpressRoute. Dedicated private network fiber connections to Azure - Traffic Manager. Route incoming traffic for high performance and availability - Load Balancer. Deliver high availability and network performance to applications - Azure DNS. Host DNS domains in Azure - VPN Gateway. Establish secure, cross-premises connectivity - Application Gateway. Highly scalable websites with HTTP load balancing and delivery control
Media and CDN	- Media Services. Encode, store, and stream video and audio at scale - Encoding. Studio Grade encoding at Cloud Scale - Azure Media Player. A single player for all playback needs - Azure Media Indexer. Enhance discoverability and accessibility of media - Content Protection. Securely deliver content using AES, PlayReady, and Widevine - Live and On-Demand Streaming. Deliver content to virtually all devices with the scale to meet business needs - CDN. Deliver content to end-users through a robust network of global data centers
Hybrid Integration	- BizTalk Services. Seamlessly integrate the enterprise and the cloud - Service Bus. Connect across private and public cloud environments - Backup. Simple and reliable server backup to the cloud - Site Recovery. Orchestrate protection and recovery of private clouds
Identity & Access Management	- Azure Active Directory. Synchronize on-premises directories and enable single sign-on - Azure Active Directory B2C. Consumer identity and access management in the cloud - Azure Active Directory Domain Services. Domain controller as a service - Multi-Factor Authentication. Safeguard access to data and apps with an extra level of

	authentication
Developer Services	- Visual Studio Team Services. Services for teams to share code, track work, and ship software - Azure DevTest Labs. Quickly create environments using reusable templates and artifacts - Visual Studio Application Insights. Diagnose problems and track usage to improve web and mobile apps - HockeyApp. Deploy mobile apps, collect feedback and crash reports, and monitor usage
Management & Security	- Microsoft Azure portal. Explore the new Microsoft Azure portal - Scheduler. Run jobs on simple or complex recurring schedules - Automation. Simplify cloud management with process automation - Operational Insights. Collect, search and visualize machine data from on-premises and cloud - Key Vault. Safeguard and maintain control of keys and other secrets - Security Center. Prevent, detect, and respond to threats with increased visibility

Scope and Variety: VMware vCloud Air

vCloud Air is a secure public cloud service operated by VMware, built on the trusted foundation of VMware vSphere. The service supports existing vSphere workloads and third- party applications as well as new application development, providing customers a common platform to seamlessly extend their data center into the public cloud and remain in control. When combined with existing vSphere data centers, vCloud Air forms a scalable, portable and agile hybrid cloud.

vCloud Air consists of three primary service offerings:

- Dedicated Cloud.** Dedicated physical infrastructure compute service
- Virtual Private Cloud.** Logically isolated, multi-tenant compute service
- Disaster Recovery.** Business continuity for on-premises environments, safe in vCloud Air.

Each service offers a variety of features and a selection of Add-Ons to meet customer needs.

Table 11: VMware vCloud Air. A secure public cloud service operated by VMware, built on the trusted foundation of VMware vSphere.

VMware vCloud Air Service	Description
Dedicated Cloud	VMware vCloud Air Dedicated Cloud is a dedicated single- tenant, physically isolated cloud IaaS that provides customers: - A broad set of capabilities among the compute services in vCloud Air - A service for migrating existing large production workloads, hosting Test/Dev environments, and developing new applications
Virtual Private Cloud	VMware vCloud Air Virtual Private Cloud is a scalable & secure public cloud infrastructure as a service solution built on the foundation of vSphere that provides customers: - Compatibility with on premises vSphere workloads to create a true hybrid solution - Support for both new and existing applications and the option to create new or migrate existing workloads and always maintain control. - A cost-effective solution for expanding business capacity to accommodate geographic and seasonal needs without building out costly data centers and suffering from underutilized resources
Disaster Recovery	VMware vCloud Air Disaster Recovery is a recovery-as-a-service (RaaS) solution that introduces native cloud-based disaster recovery capabilities for VMware vSphere virtual environments. Built on

	VMware's hypervisor-based replication engine, vSphere Replication, vCloud Air Disaster Recovery includes: • Self-service disaster recovery protection for virtual machines • Recovery point objectives (RPO) from 15 minutes to 24 hours • Readily facilitates failover, failback and planned migration as needed • Retention of multiple recovery points. up to 24 point-in-time instances • Elastic cloud compute and storage capacity • Support for offline data seeding • Private leased line network option • Flexible failover testing
Data Protection	VMware vCloud Air Data Protection offers secure, policy-based backup and recovery in the cloud for virtual machines hosted exclusively on vCloud Air. Available across both Dedicated Cloud and Virtual Private Cloud infrastructure-as-a-service types, Data Protection includes: • Backup policy affinity controls per Virtual Data Center (VDC) or per vApp • Daily (24-hour) Recovery Point Objective (RPO) guarantee • Virtual machine (image-level) Restore Granularity Objective (RGO) • Custom backup window scheduling • Configurable data retention • On-demand backups • Synthetic-full backup images • Intelligent consumption tracking and activity reports
Direct Connect	VMware vCloud Air Direct Connect is a dedicated, high-throughput networking link that connects remote data centers and those in the same colocation facility to an instance in vCloud Air. Available for Dedicated, Disaster Recovery, and Virtual Private Cloud service options, Direct Connect provides an additional connection method into vCloud Air that offers: • High throughput up to 1 or 10 Gbps • Dedicated path with low latency • Privacy and security • Support for secure multi-point connections
Advanced Networking Services	VMware vCloud Air Advanced Networking Services is a re-invented model for public cloud security that improves overall network manageability and accelerates application time- to-market by delivering a powerfully agile and cost-efficient platform for zero-trust security in the cloud. Built on VMware NSXTM technology, these services offer customers a path toward true hybrid networking
Hybrid Cloud Manager	VMware vCloud Air Hybrid Cloud Manager offers VMware vSphere users a seamless option for extending their on-premises data center into vCloud Air. Customers can extend their environments to include vCloud Air with L2 VPN network extension. More importantly, customers are able to take advantage of bi-directional workload portability, using replication-based, WAN accelerated application migration. These capabilities simplify workload management and enable users to extend their environments effectively for a true hybrid cloud experience.
Offline Data Transfer	Offline Data Transfer is a data migration service for a large numbers of VMs, vApps, or templates from a customer's local private vSphere or vCloud Director Environments to vCloud Air via physical disk. This is a faster and more economical way than migrating large amounts of data via the Internet. VMware will provide customers with a secure, encrypted physical storage device for data. Simply return this device using the mail carrier of choice and VMware will upload data to vCloud Air.

Scope and Variety: SoftLayer

SoftLayer offers one of the highest performing cloud infrastructures available—one platform that takes data centers around the world that are full of the widest range of cloud computing options, and then integrates and automates everything.

Table 12: SoftLayer. *Developed the industry's first Network-Within-a-Network topology for true out-of-band access and offers an easy-to-use customer portal and robust API for full remote-access of all product and service management options.*

SoftLayer Product or Service	Depth and Breadth
Cloud Servers	Bare Metal Servers. Ordered to customers' exact specifications via the SoftLayer portal or API and deployed in real time to any SoftLayer data center and have it online in as little as 20-30 minutes. Virtual Servers. Offer a higher degree of customization, transparency, predictability, and automation, and integrate seamlessly with SoftLayer bare metal servers. GPUs. To accelerate application and processing performance, the CPU offloads compute-intensive portions of the application to the GPU to process large blocks of data at one time—rather than sequentially—boosting the overall performance in a server environment. 32- and 64-bit Operating Systems. CentOS, CoreOS, CloudLinux, Debian, FreeBSD, Microsoft, Red Hat, Ubuntu, and Vyatta Network. Virtualization. Citrix XenServer, Parallels Cloud Server, Microsoft Hyper-V, VMware ESX and ESXi, and VMware vSphere. Security. APF Software Firewall, McAfee Total Protection, McAfee Anti-Virus, McAfee Host Intrusion Protection, Nimsoft Monitoring, and Microsoft Windows Firewall. Databases. Microsoft SQL Server (2005, 2008, 2012, 2014), MySQL, IBM Cloud Analytics, Cloudera Hadoop, MongoDB, and Basho Riak. Control Panel. cPanel/WHM with Fantastico, RVSkin and Softaculous; Parallels Plesk Panel
Cloud Storage	Object Storage. Dedicated and a highly scalable storage solution based on OpenStack Swift for organizing and managing unstructured data. Block Storage. Persistent, iSCSI-based block storage up to 12TB in capacity. Endurance block storage includes snapshot and replication capabilities and can be provisioned in one of three performance tiers to meet most block-level storage needs. Performance block storage is available for high-I/O application needs with up to 6,000 allocated IOPS per volume. File Storage. High performance, feature-rich NFS-based file-level NAS storage with file share capacities available up to 12TB. Provisioned with snapshot and replication support (Endurance) or with IOPS allocations (Performance). Mass Storage Servers. Customers may design and manage their own bare metal mass storage device with their choice of operating system or deploy OS NEXUS QuantaStor to create a turnkey storage appliance. Cleversafe Object Storage. Cleversafe provides on-premise, public cloud and hybrid cloud storage solutions that enable enterprises to take advantage of mobile, cloud, cognitive and the IoT. Content Delivery Network. SoftLayer has partnered with EdgeCast to offer one of the fastest and most reliable content delivery networks. Distribute content in 24 geographically diverse nodes to shorten the distance it has to travel to end users. Customers only pay for the bandwidth used. Backup. SoftLayer provides turnkey EVault and R1Soft automatic backup solutions, as well as the ability to create a virtual or bare metal server running customer's own backup application.
Networking	Load Balancing. Manages the traffic and resource usage of server nodes in the environment. Local, global, and high availability options can be activated, changed, and deactivated at any time.

	• Network Appliances. Creates all-in-one network appliances using software-defined networking solutions. • Direct Link. Plug into SoftLayer's private network via a Network Service Provider, Cloud Exchange Provider, or Colocation Provider for unparalleled network performance to and from the SoftLayer infrastructure.
Security	• Security Software. Complete array of Intrusion Protection Systems (IPS) and Intrusion Detection and Prevention Systems (IDPS) software for both the network and server/host level. • Firewalls. Hardware firewalls, Fortigate Security Appliance, gateway appliances, software defined firewall, router, VPN, and more. • SSL Certificates. Choose from Symantec or GeoTrust SSL certificate product offerings
Developers	• Email Delivery. Built on SendGrid, SoftLayer's email delivery service is a highly scalable email relay solution that integrates into applications and services on the SoftLayer platform. • Message Queue. Run on a full-featured, easy-to-use REST API and available for applications running on servers or on any other infrastructure at SoftLayer. • Digital Transcoding. Free service enables customers to convert audio or video assets into a wide range of sizes and formats optimized for content delivery.
Management Controls and Tools	• SoftLayer API • Customer Portal • Mobile Applications. • Monitoring & Reporting • Management Tools • Managed Hosting • Support

Requirement 6.7 (E) BEST PRACTICES

Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

Best Practices: Amazon Web Services

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and segregation. AWS's highly secure data centers use state-of-the-art electronic surveillance and multi-factor access control systems and maintain strict, least-privileged-based access authorizations. Environmental systems are designed to minimize the impact of disruptions to operations, and multiple geographic regions and Availability Zones allow customers to remain resilient in the face of most failure modes, including natural disasters or system failures. AWS manages over 1,800 security controls to provide an optimally secure environment for all of our customers.

In addition, network traffic between AWS regions, Availability Zones, and individual data centers travels over private network segments by default. These private network segments are fully isolated from the public Internet and not routable externally. AWS resources can be configured to reside only on isolated AWS network segments and to avoid utilizing any public IP addresses or routing over the public Internet.

AWS security engineers and solution architects have developed [whitepapers and operational checklists](#) to help customers select the best options for their needs and to recommend security best practices, such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.

AWS: Built-In Security Features

Applications and data are not only protected by highly secure facilities and infrastructure, but also protected by extensive network and security monitoring systems. AWS and its partners offer over 700 tools and features to help customers meet their security objectives concerning visibility, auditability, controllability, and agility. These tools and features provide basic but important security measures such as Distributed Denial of Service (DDoS) protection and password brute-force detection on AWS accounts. AWS-provided security features include:

Table 13: AWS Best Practices. Built-in Security Features.

Best Practice	Description
Secure Access	Customer access points, also called Application Programming Interface (API) endpoints, allow secure HTTP access (HTTPS) so that customers can establish secure communication sessions with their AWS cloud services using Secure Socket Layer (SSL)/Transport Layer Security (TLS).
Built-In Firewalls	Customers can control how accessible their instances are by configuring built-in firewall rules—from totally public to completely private or somewhere in between. And when instances reside within an Amazon Virtual Private Cloud (Amazon VPC) subnet, customers can control egress as well as ingress.
Unique Users	The AWS Identity and Access Management (IAM) tool allows AWS customers to control the level of access their own users have to AWS infrastructure services. With AWS IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.
Multi-Factor Authentication (MFA)	AWS provides built-in support for MFA for use with AWS accounts as well as individual AWS IAM user accounts.
Private Subnets	The Amazon VPC service allows customers to add another layer of network security to instances by creating private subnets and even adding an Internet Protocol Security (IPsec) Virtual Private Network (VPN) tunnel between a home network and Amazon VPC.
Encrypted Data Storage	Customers can have the data and objects they store in Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon Redshift, and Amazon Relational Database Service (Amazon RDS) on Oracle and SQL Server encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
Dedicated Connection Option	The AWS Direct Connect service allows customers to establish a dedicated network connection from their premises to AWS. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple logical connections to enable access to both public and private IP environments within the AWS cloud.
Isolated GovCloud	For customers who require additional measures in order to comply with US International Traffic in Arms Regulations (ITAR), AWS offers an entirely separate region called AWS GovCloud (US) . This isolated region provides an environment where customers can run ITAR-compliant applications and provides special endpoints that utilize only Federal Information Processing Standard (FIPS) 140-2 encryption.
Dedicated, Hardware-Based Crypto Key Storage Option	For customers who must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.
Centralized Key Management	For customers who use encryption extensively and require strict control of their keys, the AWS Key Management Service (KMS) provides a convenient management option for creating and administering the keys used to encrypt data at rest.

Perfect Forward Secrecy	For even greater communication privacy, several AWS cloud services such as Elastic Load Balancing and Amazon CloudFront offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use Perfect Forward Secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.

AWS: Visibility into Data, Performance, and Resource Usage

Several of AWS's built-in cloud security features focus on providing visibility into data, performance, and resource usage. The tools listed below help customers gain more insight into their cloud operations, giving them the means to better control their security and providing information for data-driven decisions.

Table 14: AWS Best Practices. Visibility into Data, Performance, and Resource Usage.

Best Practice	Description
AWS Trusted Advisor	Provided automatically when AWS customers sign up for premium support, the AWS Trusted Advisor service is a convenient way for customers to see where they could use a little more security. It monitors AWS resources and alerts customers to security configuration gaps such as overly permissive access to certain Amazon Elastic Compute Cloud (Amazon EC2) instance ports and Amazon S3 storage buckets, minimal use of role segregation using AWS IAM, and weak password policies.
Amazon CloudWatch	Amazon CloudWatch enables customers to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by a customer's applications and services and any log files their applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly.
AWS CloudTrail	AWS CloudTrail provides logs of all user activity within an AWS account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS cloud service. The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.
AWS Config	With the AWS Config service, customers can immediately discover all of their AWS resources and view the configuration of each. Customers can receive notifications each time a configuration changes as well as dig into the configuration history to perform incident analysis.

AWS: Third-Party Security Tools

AWS offers additional third-party security tools to complement and enhance customer operations in the AWS cloud. [AWS Partner Network](#) (APN) partners offer hundreds of familiar and industry-leading products that are equivalent to, identical to, or integrate with existing controls in a customer's on-premises environments. Customers can browse and purchase APN partner products on the [AWS Marketplace](#). These products complement existing AWS cloud services to enable customers to deploy a comprehensive security architecture and a more seamless experience across their cloud and on-premises environments. The APN partner security products cover multiple areas of security, including application security, policy management, identity

management, security monitoring, vulnerability management, and endpoint protection. Figure 1 is a snapshot of the APN partners and categories of products available under the security category in the AWS Marketplace.



Figure 1: The AWS Marketplace provides access to many familiar and trusted security vendors.

Several of the security products that AWS offers are provided only by APN partners that are prequalified by the [APN Partner Competency Program](#), which confirms their technical proficiency and proven customer success in specialized solution areas. AWS's [Security Competency Partners](#) can also provide demos and consulting services that are not always available through the AWS Marketplace.

Best Practices: Microsoft Azure

Microsoft believes customers want to retain control of their data—and they want that data to be kept secure and private while maintaining transparency and compliance. The following sections describe Microsoft's best practices, policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services.

Microsoft Azure: Security Design and Operations

Azure cloud services are designed for security from the ground up. Microsoft's secure cloud solutions are the result of comprehensive planning, innovative design, and efficient operations—from code development to incident response. Code development adheres to a software development process that embeds security requirements into systems and software through the planning, design, development, and deployment phases.

Table 15: Microsoft Best Practices. Security Design and Operations.

Best Practice	Description
Enhanced Operational Security	A rigorous set of security controls govern operations and support—protecting Azure against unauthorized developer and/or administrative activity by deploying preventive, defensive, and reactive controls such as: • Requiring two-factor smartcard-based authentication to perform sensitive operations; • Controls that enhance independent detection of malicious activity; • Multiple levels of monitoring, logging, and reporting; and • Limiting operations personnel access to applications, systems, and network infrastructure in proportion to the required level of background verification.
Assume Breach	Microsoft's strategy, "Assume Breach", stays ahead of emerging threats and hardens its cloud services. By simulating real-world attacks at the network, platform, and application layers, software security experts assess Azure's ability to detect, protect against, and recover from breaches.
Incident Management and Response	Microsoft's global, 24x7 incident response service mitigates the effects of attacks and malicious activity by following established procedures for incident management, communication, and recovery. In the event of a security incident, Microsoft's incident response team will: • Identify the security issue, assign a severity classification and escalated it appropriately; • Contain the incident to ensure data is safe; • Eradicate any damage and identify the root cause of the security issue; • Apply software or configuration updates to the system and return services to full working capacity; and • Analyze the incident to ensure the appropriate mitigations are applied to protect against future recurrence.

Microsoft Azure: Visibility, Compliance, Data Security and Threat Protection

Microsoft has a number of policies and procedures to ensure visibility, compliance, data security and threat protection for cloud-delivered services.

Table 16: Microsoft Best Practices. Visibility, Compliance, Data Security and Threat Protection.

Best Practice	Description
Infrastructure Protection	Microsoft addresses security risks across Azure's infrastructure—the hardware, software, networks, administrative and operations staff, and the physical data centers that house it all.
Network Protection	Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Because Azure's shared infrastructure hosts hundreds of millions of active VMs, protecting the security and confidentiality of network traffic is critical. In the traditional datacenter model, the IT organization controls networked systems, including physical access to networking equipment. In the cloud service model, the responsibilities for network protection and management are shared between the cloud provider and the customer. Customers do not have physical access, but they implement the logical equivalent within their cloud environment through tools such as Guest operating system (OS) firewalls, Virtual Network Gateway configuration, and Virtual Private Networks.
Data Protection	Azure allows customers to encrypt data and manage keys, and safeguards customer data for

	applications, platform, system and storage using three specific methods: encryption, segregation, and destruction.
Identity and Access	Microsoft has strict controls that restrict access to Azure by Microsoft employees. Azure also enables customers to control access to their environments, data and applications.
Privacy	Microsoft builds and operates products and services to protect privacy. Standards and processes supporting these principles include detailing Microsoft's core privacy requirements and practices, addressing privacy requirements throughout development lifecycle, contractual commitments to safeguard customer data, as well as compliance with international standards. Microsoft uses customer data stored in Azure only to provide the service, including purposes compatible with providing the service. Azure does not use customer data for advertising or similar commercial purposes.
Customer Control of Data	Microsoft alleviates the fear of losing control that causes an customer's decision makers to hesitate by making a clear commitment to provide customers with control over their data.
Transparency	To effectively exercise their right to control their data, Azure customers have access and visibility to that data, know where it is stored, and—through clearly stated and readily available policies and procedures—how Azure helps secure customer data, who can access it, and under what circumstances.
Conformity to Global Standards	The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve in the future. It also makes it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft to maintain and expand its portfolio of third-party certifications. These help customers demonstrate compliance readiness to their customers, auditors, and regulators. As part of its commitment to transparency, Microsoft shares third-party verification results with its customers.

Best Practices: VMware vCloud Air

vCloud Air can deliver end-to-end hybrid cloud security by using common technology and operational models between the on-premises data center and the public cloud.

VMware vCloud Air: Cloud Computing Security

Since the reach of IT Security does not have to end where the public cloud begins, VMware enables customers to:

- Extend trusted IT security frameworks to the cloud
- Embed security policies to follow workloads anywhere
- Build cloud infrastructure based on data center standards

Table 17: VMware Best Practices. Cloud Computing Security.

Best Practice	Description
Control	vCloud Air extends IT Security control across hybrid environments: - Protect data and secure access through network isolation policies and granular security controls—regardless of on or offsite workload locations - Leverage trusted protocols and tools to reduce the risk of security incidents and compliance deficiencies
Portability	vCloud Air meets the dynamic security demands of extending data centers to the public cloud with portable protection: - Extend trusted security frameworks across hybrid boundaries of a multi-tenant environment - Embed security controls into workloads, data and applications that stay with them regardless of where they reside or move
Consistency	vCloud Air securely extends data centers on a public cloud platform built from the ground up to the customer's exact production standards: - Expand the boundaries of current policies and controls by replicating existing network constructs to reduce risk and create scalable protection - Maintain consistency in managing the confidentiality, integrity and availability of data across hybrid infrastructure

VMware vCloud Air: Visibility, Compliance, Data Security and Threat Protection

Microsoft has a number of policies and procedures to ensure visibility, compliance, data security and threat protection for cloud-delivered services.

Table 18: VMware Best Practices. Visibility, Compliance, Data Security and Threat Protection.

Best Practice	Description
vCloud Air Shared Responsibility Model	Trusted security in the cloud is achieved through the partnership of shared responsibilities between customers and vCloud Air. vCloud Air secures the underlying infrastructure of the data center location with tenancy isolation, timely catalog OS patches, user access controls and documented certifications and audits. Customers continue to own and operate the security and compliance of the actual workloads by extending their successful policies and controls to their offsite public cloud locations. And trusted partners now offer increased innovations, best practice implementation reference architectures and purpose-built virtual appliance delivery methods to increase the manageability and consistency of security across a hybrid infrastructure. This partnership empowers businesses to achieve increased effectiveness in their ability to mitigate risks to their data sets in the public cloud.
Cloud Compliance and Security	VMware is committed to delivering a cloud service that adopts industry best practices in order to meet a comprehensive set of international and industry specific security and compliance standards. VMware adheres to rigorous security standards and is rapidly expanding coverage for various industry-specific security and compliance measures. VMware makes independent third-party examination and audit reports available to customers that will satisfy a wide range of customer specific compliance requirements.
Managing Security Threats	For the very same reason—server consolidation—virtualization has both revolutionized the data center and become a target for attackers to gain access to confidential data, VMware protects the vCloud Air platform from the impacts of malicious activity by addressing various security threats.

Physical and Logical Security	The vCloud Air Virtual Private Cloud (VPC) offering is a logically isolated set of resources with its own internal network and a virtual network Edge Gateway where customers can set up their own firewall and NAT rules. Network segmentation is achieved through virtual extensible LANs (VxLANs) allowing for a large range of isolated networks for customers. Customers can connect to their virtual machines over IPsec VPN tunnels. The vCloud Air Dedicated Cloud offering provides physically isolated and reserved compute resources from all other vCloud Air tenants, paired with one or more virtual network Edge Gateways where customers can set up their own firewall and NAT rules. Network segmentation is achieved through VxLANs allowing for a large range of isolated networks for customers. Customers can connect to their VMs over IPsec VPN tunnels.

Best Practices: SoftLayer

SoftLayer believes cloud computing is not a commodity because no two clouds are built the same way. The following sections describe SoftLayer's best practices, policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services.

SoftLayer: Multi-Layer Security Strategy

SoftLayer's multi-layer security strategy protects its customers from malicious activity and mitigates risks with respect to data, customer information, uptime, and potentially the customer's reputation. SoftLayer provides unique networks to segregate public, private, and management traffic across distinct physical networks and offers a broad selection of industry-leading hardware and software solutions to help customers create a comprehensive strategy.

Table 19: SoftLayer Best Practices. Multi-Layer Security Strategy.

Best Practice	Description
Physical and Operational Security	Because there can be many points of entry or attack for malicious activity, SoftLayer provides a wide range of security options to choose from. Customers can protect their infrastructure with multiple, overlapping layers of protection customized to their needs and interests.
Network Security	SoftLayer's innovative network architecture and commitment to using the most advanced hardware technologies dramatically minimizes data center and server exposure to outside threats. The network integrates three distinct and redundant architectures into a multi-tiered network topology. Systems are fully accessible to customer administrative personnel but safely off-limits to others.
System, Application, and Data Security	Beneath layers of physical and network protection, Several tiers of comprehensive, standard security features safeguard customer computing systems, applications, and data. Additional hardware-assisted security options are available on demand, allowing customization of an enterprise's security profile based on changing requirements or client needs.

SoftLayer: Visibility, Compliance, Data Security and Threat Protection

Microsoft has a number of policies and procedures to ensure visibility, compliance, data security and threat protection for cloud-delivered services.

Table 20: SoftLayer Best Practices. Visibility, Compliance, Data Security and Threat Protection.

Best Practice	Description
Data Centers	Every aspect of a SoftLayer data center—from location and accessibility to power density and redundancy—is designed to guarantee its security, resiliency, and efficiency. And each is staffed 24x7 with experts to troubleshoot and address the rare issues that can't be directly resolved through our automated management system. SoftLayer builds each data center to the same spec and equips it to provide the full SoftLayer catalog of services.
Network	Our data centers are connected by the industry's most advanced network within a network, which integrates distinct public, private, and internal management networks to deliver lower total networking costs, better access, and higher speed. Public, private, and management traffic travel across separate network interfaces, segregating and securing traffic while streamlining management. Our global network boasts more than 2,000Gbps of connectivity between data centers and network points of presence (PoPs). These locations each have multiple 10Gbps transit connections as well as peering links to additional service providers and access networks.
Automation	Our data centers and network share a single, proprietary management system. One tool that ties together and lets customers control everything—every bare metal server, virtual server, storage device—in a single pane of glass. All accessible by API, portal, and mobile applications. If we can't automate it, we don't offer it. Every offering on our platform—from servers and storage to firewalls, load balancers, and even our accounting system—is controlled by a single management system with its own API. We've automated the deployment and management of everything. And we extend total access and control to customers through the same API, as well as through an easy-to-use Web portal and mobile applications.
Security Hardware and Software	SoftLayer offers its customers a complete array of solutions to protect servers and applications with unique security hardware and software throughout their environment. Customers can monitor for, and respond to, security threats with in-depth scanning and logging capabilities and stay up-to-date with patches and security updates for supported operating systems and software.
SSL Certificates	SoftLayer offers Secure Socket Layer (SSL) certificates to provide a secure, encrypted connection between customer sites or applications and their end users. SoftLayer partners with the most respected providers in the security industry so customers may choose SSL certificates that best meets their needs. Customers manage their SSL certificates quickly and easily in the SoftLayer customer portal.
Compliance with Industry Standards	Because the physical and virtual controls of SoftLayer's facilities, network, and customer portal are an extension of their own, customers require access to reports and information for their own compliance needs. SoftLayer's compliance department works with independent auditors and third-party organizations to meet the industry's most stringent guidelines and makes it easy for customers to get the information they need for their own audits.
Management Controls and Tools	Using SoftLayer's fully automated platform, customers can directly manage their own infrastructure and do anything that a SoftLayer team member can do—except for going into the data center themselves. Should customers focus their time and resources on core competencies, SoftLayer has a team of managed hosting experts ready to help manage their infrastructure. Customer choose from the management services that meet their business needs—from DIY tools to a dedicated team. Management services are completely integrated and available 24x7—customers have 'round-the-clock access to the tools and support resources they need to manage bare metal and virtual servers.
Support and Managed Hosting Services	SoftLayer's self-service knowledgebase, community-driven forums, or helpful technical support department provide customers all the information they need to keep their environments up and running securely. SoftLayer support is available 24x7x365 to help customers resolve issues. All



	SoftLayer products include unlimited access to expert technical support at no additional charge. When providing full-service support, SoftLayer staff will confirm that the product or service is working as originally delivered and provide general guidance. Unfortunately, we cannot make configuration changes, manipulate customer data, or customize the product or service. Customers are responsible for supporting their own data, third-party software, customer-owned devices, and offsite servers and services. SoftLayer's managed hosting is dedicated team of certified engineers and cloud experts available 24x7 to manage core services including database, security, monitoring, and backup. Best for large, multi-faceted deployments, the SoftLayer managed hosting team get solutions up and running as soon as possible.

Section Title: Organization Profile

This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.

7 ORGANIZATION AND STAFFING

Requirement 7.1 (ME) CONTRACT MANAGER

The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. The Contract Manager must have experience managing contracts for cloud solutions.

Requirement 7.1.1

Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.

Name	James Flint
Phone	703-635-2616
Email	jflint@emergent360.com
Work Hours	8:30-5:30 EST

Requirement 7.1.2

Describe in detail the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. Provide a detailed resume for the Contract Manager.

Since being hired in 2010, Mr. Flint has led Emergent's contract management operations, established new manufacturer relationships, and responded to strategic contract vehicle solicitations.

Work Experience

Prior to joining Emergent, he had an accomplished tenure other public sector Value-Added Resellers, including GTSI Corp. (now Unicom Government, Inc.) and immixGroup. His accomplishments included:

- ✓ Developing a strong understanding of the relationships of the Value-Added Reseller marketplace, OEM's, and federal customers.
- ✓ Establishing a program management plan for immixGroup while revamping existing contract management processes and systems to produce daily technology refreshment proposals (TRs) and order fulfillment processes to track orders through shipment and delivery.
- ✓ Developing immixGroup into a consistent performer and maintaining excellent performance ratings for a first-time holder of multi-billion dollar federal Information Technology IDIQ by educating all of immixGroup's staff—including senior executives—and manufacturer

partners on how to best utilize it (NASA's Solution for Enterprise Wide Procurement or "SEWP")

- ✓ Establishing a process to quickly identify, engage, and onboard manufacturers as a means to bring more OEMs to SEWP and to feed immixGroup's own pipeline of partners.
 - This contributed to increasing the number of immixGroup manufacturer reseller agreements from approximately 65 to over 200
- ✓ Regularly volunteering and participating on various industry panels.
- ✓ Led immixGroup's to achieve a company-wide ISO 9001:2000 registration.

Since arriving at Emergent, Mr. Flint has:

- ✓ Established Emergent's Contract Management PMO and Quality Management System to oversee all Emergent contract operations.
- ✓ Managed Emergent's efforts to increase the number of manufacturer partners and reseller agreements from approximately 12 to over 90.
- ✓ Developed processes and internal automated systems to manage contracts and prepare daily contract modifications across all contracts.
- ✓ Acquired and novated a multi-billion dollar federal contract, NIH's Electronic Commodity Store III (ECS III), and initiated business development efforts surrounding it.
- ✓ Led Emergent's parent company's services organization, Mythics Consulting, to an ISO 9001:2008 registration.

Since 2010, Mr. Flint has refined and improved our internal systems, processes and procedures in preparation for managing contracts of similar size and scope as NASPO, in terms of volume and magnitude as described in the appropriate sections within this proposal.

Education

- In 1991, Mr. Flint received a B.S. in Computer Science from the College of William and Mary in Williamsburg, VA.
- In 1997, Mr. Flint received a M.S in Information Systems Management from the American University in Washington D.C.
- In 2009, Mr. Flint received a M.B.A. from George Mason University in Fairfax, VA.

Requirement 7.1.3

Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

Responsible for overall program performance and customer satisfaction, Mr. Flint directs all Emergent administrative and operational functions and is the primary point of contact through which communications flow between Emergent, NASPO/ValuePoint, and the State of Utah. Overseeing our quality assurance program, Mr. Flint implements, maintains, and promotes awareness of all quality initiatives specific to program requirements and continuously measures, evaluates, and improves performance.

Mr. Flint will also:

- Provide open and centralized communication with NASPO/ValuePoint and the State of Utah

-
- Work with States where Emergent has existing contracts to transition them to NASPO/ValuePoint
 - Meet with NASPO/ValuePoint and the State of Utah to address any outstanding items during the course of the contract
 - Ensure eligible entities understand how to best utilize the contract
 - Ensure overall customer satisfaction by working closely with Emergent's Customer Excellence Team
 - Work closely with the Emergent's Marketing Team to identify new marketing opportunities; promote our proposed CSPs and their solutions; and identify any gaps in current marketing strategy
 - Work closely with the Emergent Sales Teams to ensure staff are trained, engaged and committed to the NASPO/ValuePoint program

Section Title: Technical Response

This section should constitute the Technical response of the proposal and must contain at least the following information:

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

8 TECHNICAL REQUIREMENTS

If applicable to an Offerors offering, an Offeror must provide a point by point responses to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's offering then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

FedRAMP: Applicable Requirements, Standards, and Guidance

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Goals and Objectives	✓ Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations ✓ Increase confidence in security of cloud solutions ✓ Achieve consistent security authorizations using a baseline set of agreed upon standards to be used for cloud product approval in or outside of FedRAMP ✓ Ensure consistent application of existing security practice ✓ Increase confidence in security assessments ✓ Increase automation and near real-time data for continuous monitoring
Benefits of Authorization	✓ Increase re-use of existing security assessments across agencies ✓ Save significant cost, time, and resources—"do once, use many times" ✓ Improve real-time security visibility ✓ Provide a uniform approach to risk-based management ✓ Enhance transparency between government and Cloud Service Providers (CSPs) ✓ Improve the trustworthiness, reliability, consistency, and quality of the Federal security authorization process

The most current approved version of the following requirements, standards, and guidance in **Table 21** below are applicable to the FedRAMP program, regardless of the version noted.

Table 21: FedRAMP Requirement, Standards, and Guidance. *One of the benefits of receiving FedRAMP Authorization is significant savings in terms of cost, time, and resources—"do once, use many times".*

Guidance	Topic
FIPS Publication 199	<i>Standards for Security Categorization of Federal Information and Information Systems</i>
FIPS Publication 200	<i>Minimum Security Requirements for Federal Information and Information Systems</i>
NIST SP 800-18, Revision 1	<i>Guide for Developing Security Plans for Federal Information Systems</i>
NIST SP 800-27, Revision A	<i>Engineering Principles for Information Technology Security (A Baseline for Achieving Security)</i>
NIST SP 800-30, Revision 1	<i>Guide for Conducting Risk Assessments</i>
NIST SP 800-34, Revision 1	<i>Contingency Planning Guide for Federal Information Systems</i>
NIST SP 800-37, Revision 1	<i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i>
NIST SP 800-39	<i>Managing Information Security Risk: Organization, Mission, and Information System View</i>
NIST SP 800-53, Revision 4	<i>Security and Privacy Controls for Federal Information Systems and Organizations</i>
NIST SP 800-53A, Revision 4	<i>Assessing Security and Privacy Controls for Federal Information Systems and Organizations</i>
NIST SP 800-60, Revision 1	<i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>
NIST SP 800-61, Revision 2	<i>Computer Security Incident Handling Guide</i>
NIST SP 800-64, Revision 2	<i>Security Considerations in the System Development Life Cycle</i>
NIST SP 800-115	<i>Technical Guide to Information Security Testing and Assessment</i>
NIST SP 800-128	<i>Guide for Security-Focused Configuration Management of Information Systems</i>
NIST SP 800-137	<i>Information Security Continuous Monitoring for Federal Information Systems and Organizations</i>
NIST SP 800-145	<i>The NIST Definition of Cloud Computing</i>
NIST SP 800-46	<i>Cloud Computing Synopsis and Recommendations</i>

Requirement 8.1 (M)(E) TECHNICAL REQUIREMENTS

Requirement 8.1.1

Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.

- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 6.5.3 with respect to **Table 8** identifying the service models, deployment models, and risk category for each of our proposed CSPs.

- ✓ Please see Emergent's response to Requirement 6.6 with respect to the scope and variety of the solutions we have proposed to offer under this solicitation.
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
- ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Requirement 8.1.2

For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the following characteristics, as defined in NIST Special Publication 800-145:

Emergent's proposed SaaS, PaaS, and IaaS offerings possess all NIST Essential Characteristics of Cloud Computing.

Table 22: NIST Essential Characteristics of Cloud Computing. *Emergent's proposed SaaS, PaaS, and IaaS offerings all meet the guidelines of NIST SP 800-145.*

CSP	On-Demand Self-Service	Broad Network Access	Resource Pooling	Rapid Elasticity	Measured Service
	Provision services without assistance?	Available over the network?	Multi-tenant model?	Provision and release services?	Manage resource usage?
Amazon Web Services	✓	✓	✓	✓	✓
Microsoft Azure	✓	✓	✓	✓	✓
VMware vCloud Air	✓	✓	✓	✓	✓
SoftLayer	✓	✓	✓	✓	✓

Requirement 8.1.2.1

NIST Characteristic - On-Demand Self-Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.

Amazon Web Services AWS provides on-demand delivery of IT resources and application via the internet with a pay-as-you-go pricing. AWS resources can be provisioned or de-provisioned on-demand from the AWS management console. Computing resources are made available immediately upon request – the lapse time typically is for the provisioned resource to be on-line. Examples of such service from AWS Include Email, Applications, Network, Load-balancers, Queue Services, HSM, Compute, Storage etc.

Microsoft Azure Microsoft provides Availability on Demand IN CLOUD environments, to harness a near unlimited amount of compute and storage in the cloud for dev/test, cloud bursting, migration, reporting/analytics, recovery, backup and

long-term data retention.

VMware vCloud Air	VMWare vCloud Air provides on demand self service for Cloud instances along with a self service sign up capability.
SoftLayer	IBM Softlayer provides users with an on-demand provisioning and De-provisioning of compute service with ability to scale up or down based on workloads.

Requirement 8.1.2.2

NIST Characteristic - Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided.

Amazon Web Services	AWS services are accessible from the Internet and from private networks via dedicated tunnels. AWS allows for access from any where in the world for both resource availability and administration. AWS also allows for broad access through web browsers, CUI, Mobile apps on a variety of platforms including windows, Ios and Linux from Desktops, servers, laptops, tablets and other mobile devices.
Microsoft Azure	Microsoft Azure cloud instances can be accessed through a variety of network access and is broadly available. Typical connections to the Azure instances can be made through the internet, VPN, leased lines via laptops, desktops, servers and mobile devices.
VMware vCloud Air	VMware vCloud Air can be accessed through the Internet, intranet, dedicated leased lines and at Co-lo with cross over cables. This broad network access capability can be configured based on the end users needs
SoftLayer	The SoftLayer private network facilitates complete control over server management while adding convenient and secure services. Public or Private Cloud, on premises or off-premises infrastructure, IBM has technology to allow ubiquitous access to resources. VPN to VLAN makes true out-of-band management possible through a distinct stand-alone third carrier over the SSL, PPTP or IPSEC VPN gateway.

Requirement 8.1.2.3

NIST Characteristic - Resource Pooling: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met.

Amazon Web Services	AWS pools resources to provision requested number of compute units using a multi tenant model; different physical and virtual resources are allocated dynamically based on demand. AWS leverages resource pooling to build economies of scale and cost savings. Different methodologies and technologies are used to execute resource pooling. EC2 hypervisors for example use Zen, SDN is a custom AWS solution and S3 typically offers unlimited storage for end users however disks are pooled and encrypted to user's accounts.
Microsoft Azure	Azure is enabled by broader Virtualization that treats compute, storage and networking as a homogeneous resource pool and takes advantage of highly automated processes for operating the system; hosted application servers that have near-infinite scalability resulting from the large resource pools they rely on; Azure combines large pools of compute (commodity servers), networking and storage resources into a utility computing environment from which customers can draw resources on
VMware vCloud Air	VMware hypervisor is extensively used to configure Processor, ability to memory and storage with the Additionally, vSphere workloads can be run on demand.
SoftLayer	The SoftLayer platform has role based access and depending on the application requirements or consumer need, each providers is compared, solution created, Build of Material assembled, and an approved order placed, resources provisioned and manage multi-provider billing with chargeback and showback. The abstraction from infrastructure resources is provided, and the infrastructure used based on application requirements.

Requirement 8.1.2.4

NIST Characteristic - Rapid Elasticity: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met.

Amazon Web Services	AWS allows for rapid provisioning, scale up and scale down capability based on resource utilization. As in the case with S3, AWS Offers unlimited storage and add disk arrays based on consumption and forecasts. AWS also allows rapid provisioning of other computing resources like ECF2, SQS, ELB, Workspaces etc.
Microsoft Azure	Azure implements elasticity by controlling the number of web and worker role instances that are deployed; which is leveraged to increase the number of compute resources as needed - on-demand. Azure lets the end users decide the level for elasticity: for individual tenants, groups of tenants, or for all of the

tenants based on elements of the application, such as roles, storage, queues, and caches.

VMware vCloud Air	VMware solutions allows customers to burst cloud instances on demand with the ability to add vCPU, memory and disk to any running machine.
SoftLayer	SoftLayer offers a scalable and elastic cloud infrastructure. The ability to quickly provision resources to accommodate a burst of traffic and then de-provision as resources and needs reduce is offered in the environment. The customer has the option to integrate to full featured API to have a customer preferred tool provide auto-scale function. Rapid elasticity is the integral part of the cloud services.

Requirement 8.1.2.5

NIST Characteristic - Measured Service: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.

Amazon Web Services	AWS offers a pay-as-you-go model with a billing model which requires payment for only those services used by the end user. Most IaaS and PaaS services are billed on consumption, services such as workspaces and email are measured based on maximum parameters per defined time.
Microsoft Azure	Microsoft allows for on-demand use and billing based on consumption. Azure also has provisions for longer-term contracts.
VMware vCloud Air	VMware provides the capability to include services that are metered and un-metered based on customer requirements
SoftLayer	SoftLayer allows agencies to meter services and appropriate use of services. The platform can be used to monitor, control and report on utilization of services from cloud services providers such as AWS, Microsoft Azure and VMware vCloud. The powerful billing capabilities allows customers to account for resource usage and make it auditable

Requirement 8.1.3

Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Table 23 below maps the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Table 23: Service Model Subcategories. *Our proposed CSPs provide a wide range of SaaS, PaaS, and IaaS offerings.*

Service Model/Subcategory	Amazon Web Services	Microsoft Azure	VMware vCloud Air	SoftLayer
IaaS: Computer/Infrastructure Services/Operating systems	Yes	Yes	Yes	Yes
IaaS: Computer/Infrastructure Services/Hypervisors	Yes	Yes	Yes	Yes
IaaS: Disaster Recovery/Business Continuity	Yes	Yes	Yes	Yes
IaaS: Disaster Recovery/High Availability / Failover	Yes	Yes	Yes	Yes
IaaS: GIS	Yes	Yes	Marketplace	Marketplace
IaaS: Storage/File	Yes	Yes	Yes	Yes
IaaS: Storage/Block	Yes	Yes	Yes	Yes
IaaS: Storage/Object	Yes	Yes	Yes	Yes
IaaS: Storage/Archive	Yes	Yes	Yes	Yes
IaaS: Storage/Cache	Yes	Yes	Yes	Yes
IaaS: Storage/Content Delivery Networks (CDN)	Yes	Yes	Yes	Yes
IaaS: Storage/Litigation Hold	Yes	Yes	Yes	Marketplace
IaaS: Network/Virtual network	Yes	Yes	Yes	Yes
IaaS: Network/Load balancer	Yes	Yes	Yes	Yes
IaaS: Network/DNS	Yes	Yes	Yes	Yes
IaaS: Network/Gateway (e.g. VPN or Application)	Yes	Yes	Yes	Yes
IaaS: Network/Firewall	Yes	Yes	Yes	Yes
IaaS: Network/Traffic manager	Yes	Yes	Yes	Yes
IaaS: Network/Direct link	Yes	Yes	Yes	Yes
IaaS: PC/Desktop "aaS"	Yes	Yes	Yes	Marketplace
IaaS: Security/Identity & Access Management	Yes	Yes	Yes	Yes
IaaS: Security/Encryption	Yes	Yes	Yes	Yes
IaaS: Security/Data Loss Prevention (DLP)	Yes	Yes	Yes	Yes
IaaS: Security/Web Security	Yes	Yes	Yes	Yes
IaaS: Security/Email Security	Yes	Yes	Yes	Yes
IaaS: Security/Network Security	Yes	Yes	Yes	Yes
IaaS: Security/Security Information and Event Management (SIEM)	Yes	Yes	Yes	Yes
IaaS: Security/Intrusion Management	Yes	Yes	Yes	Yes
IaaS: Security/DDOS Monitoring / Management	Yes	Yes	Yes	Yes
IaaS: Other (identify additional sub-categories and/or descriptors)	Yes	Yes	Yes	Yes
PaaS: Analytics/Hadoop	Yes	Yes	Yes	Yes
PaaS: Analytics/Business Intelligence	Yes	Yes	Marketplace	Marketplace
PaaS: Analytics/Data Warehouse	Yes	Yes	Yes	Yes
PaaS: Database/Relational	Yes	Yes	Yes	Yes
PaaS: Database/NoSQL	Yes	Yes	Yes	Yes

PaaS: Development, Testing and Deployment/Containers	Yes	Marketplace	Yes	Yes
PaaS: Development, Testing and Deployment/Services and APIs	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Mobile	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Internet of Things	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Tools	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Runtime environments	Yes	Yes	Yes	Yes
PaaS: Electronic Records Management	Marketplace	Marketplace	Marketplace	Yes
PaaS: E-Discovery	Marketplace	Marketplace	Marketplace	Yes
PaaS: GIS	Marketplace	Marketplace	Marketplace	Yes
PaaS: Integration (iPaaS)	Yes	Yes	Yes	Yes
PaaS: Open Source	Yes	Yes	Yes	Yes
PaaS: Other (identify additional sub-categories and/or descriptors)	Gaming, Mobile, Desktop	Marketplace	Marketplace	Yes
SaaS: Data Analytics	Yes	Yes	Marketplace	Yes
SaaS: Business Intelligence	Yes	Yes	Marketplace	Yes
SaaS: Business Continuity/Disaster Recovery	Yes	Yes	Marketplace	Yes
SaaS: Cloud and Infrastructure Management Tools	Yes	Yes	Marketplace	Yes
SaaS: Collaboration	Marketplace	Yes	Marketplace	Yes
SaaS: Customer Relationship Management	Marketplace	Yes	Marketplace	Yes
SaaS: Citizen Relationship Management	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Data Management	Yes	Yes	Marketplace	Yes
SaaS: E-Discovery	Marketplace	Marketplace	Marketplace	Yes
SaaS: Electronic Records Management	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace
SaaS: ERP/HR	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Finance	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Budget	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Procurement	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace
SaaS: GIS	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Human Resource/Payroll	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Human Resource/Time, Attendance and Scheduling	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Human Resource/Recruitment and Hiring	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Internet Filtering	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Licensing and Registration Systems	Marketplace	Yes	Marketplace	Yes; also in

				Marketplace
SaaS: Office Productivity/Word Processing	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Document Tracking	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/E-mail	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Spread sheets	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Presentation	Yes	Yes	Marketplace	Yes
SaaS: Message Filtering	Yes	Yes	Marketplace	Yes
SaaS: Meeting Planning, hosting, conferencing	Marketplace	Yes	Marketplace	Yes
SaaS: Mobile Data Management	Marketplace	Yes	Marketplace	Yes
SaaS: Point of Sale (POS)	Yes	Yes	Marketplace	No
SaaS: Procurement Systems	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Project and Portfolio Management (PPM) Tools.	Marketplace	Yes	Marketplace	Yes
SaaS: Security	Yes	Yes	Yes	Yes
SaaS: Travel Management	Marketplace	Yes	Marketplace	Marketplace
SaaS: Workflow and Electronic Signature	Marketplace	Yes	Marketplace	Marketplace
SaaS: Other (identify additional sub-categories and/or descriptors)	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace

Requirement 8.1.4

As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

As a responsible contract holder of public sector information technology contract, Emergent is obligated and committed to identifying and representing cloud offerings compliant with the requirements found in Attachments C and D—now and in the future.

Emergent is a significant supplier of information technology products and services to the public sector. We hold direct contracts with the most prestigious and respected federal IT procurement vehicles—known as Government-wide Acquisition Contracts (GWACs), specifically:

- ✓ NASA's Solutions for Enterprise-wide Procurements V (SEWP V)
- ✓ NIH's Chief Information Officer – Commodities and Solutions (CIO-CS)

SEWP and CIO-CS were both awarded in 2015. Each GWAC is a ten-year multi-billion dollar program eligible to ALL federal agencies and specifically mandated by Congress for the procurement of information technology and related services—including SaaS, PaaS, and IaaS.

Emergent not only resells cloud service offerings, we help our customers get into the cloud faster because we understand these and other cloud computing requirements. Based upon guidance provided by Emergent, at no charge, Federal CSOs have leveraged existing FedRAMP agency ATOs to significantly reduce implementation and deployment cycles.

Requirement 8.1.5

As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 6.5.3 with respect to **Table 8** identifying the service models, deployment models, and risk category for each of our proposed CSPs.
- ✓ Please see Emergent's response to Requirement 6.6 with respect to the scope and variety of the solutions we have proposed to offer under this solicitation.
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
- ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Requirement 8.2 (E) SUBCONTRACTORS

Offerors must explain whether they intend to provide all cloud solutions directly or through the use of subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractor do not need to comply with Section 6.3.

Requirement 8.2.1

Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Emergent does not intend on using subcontracts to perform contract requirements.

Requirement 8.2.2

If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

Should Emergent decide to work with subcontractors, the work is likely to be limited to performing light professional services to assist Purchasing Entities in deploying their cloud solutions. In such cases, the subcontractor would be performing a role that is rather narrow.

In any event, Emergent would subcontract with, and flow down the applicable terms and conditions of the Master Agreement to, any partner prior to their engagement with Participating Entity as an agent of our contract.

Requirement 8.3 (E) WORKING WITH PURCHASING ENTITIES

Requirement 8.3.1

Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;);
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

In good faith, Emergent is committed providing a description of CSP notification processes. However, Emergent also understands that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data. **Table 24** below provides publicly available information with respect to handling incidents. Breach notifications account for, and may be hindered by, applicable federal, state, and local laws in conjunction with regulatory compliance and other contractual commitments, including ISO/IEC 27001 and NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*.

Table 24: Incident Response Procedures. A host of factors contribute to the lack of detail provided in the public domain.

CSP	Incident Response Procedures
Amazon Web Services	The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution. In the event of a security incident: • Documentation is maintained to aid and inform operations personnel in handling incidents or issues. • If the resolution of an issue requires collaboration, a conferencing system is used which supports communication and logging capabilities. • Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. • Post-mortems are convened after any significant operational issue, regardless of external impact, and Cause of Error (COE) documents are drafted so the root cause is captured and preventative actions are taken in the future. • Implementation of the preventative measures is tracked during weekly operations meetings.
Microsoft Azure	Microsoft's global, 24x7 incident response service mitigates the effects of attacks and malicious activity by following established procedures for incident management, communication, and recovery. In the event of a security incident, Microsoft's incident response team will: • Identify the security issue, assign a severity classification and escalated it appropriately; • Contain the incident to ensure data is safe; • Eradicate any damage and identify the root cause of the security issue; • Apply software or configuration updates to the system and return services to full working capacity; - and Analyze the incident to ensure the appropriate mitigations are applied to protect against future recurrence.
VMware vCloud Air	VMware provides security incident response (e.g., detection, severity/threat classification, forensics, and resolution) with respect to the management infrastructure over which VMware has direct, administrative, and/or physical access and control.

	Per NIST 800-61 guidelines, VMware provides security incident response consisting of, but not limited to, the detection, severity/threat classification, systems and network forensics, recommendations and lessons learned. VMware will use commercially reasonable efforts to notify all relevant parties, taking into account any applicable law, regulation, or governmental request should VMware determine there has been unauthorized access to, use or disclosure of 'customer content', or other incident.
SoftLayer	SoftLayer's Event Management System is a toolset that optimizes the way information is shared with users about unplanned infrastructure issues and upcoming planned maintenance events. It utilizes targeted, subscription-based email alerts for these incidents to share the type of event that has occurred and provide subscribed users with additional details about the overall impact of the event and a current status of the unplanned incident in progress (UIP).

ISO/IEC 27001

Each of our proposed CSPs are audited to the ISO/IEC 27001 standard which offers best practice recommendations on information security management, risks and controls provides a framework for policies and procedures that include all legal, physical, and technical controls involved in an organization's information risk management processes. The international acceptance and applicability of ISO/IEC 27001 makes it one of the most widely recognized certifications for a cloud service.

Certifying to ISO/IEC 27001 means specific requirements are mandated, defining how to implement, monitor, maintain, and continually improve. It also specifies a set of best practices that include requirements for documentation, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures.

The applicability of complying with the ISO/IEC 27001 standard with respect to this NASPO requirement is the guidance it provides for managing information security incidents, business continuity, and compliance at:

- A.13 Information Security Incident Management (see **Table 25**)
- A.14 Business Continuity Management (see **Table 26**)
- A.15 Compliance (see **Table 27**)

Table 25: A.13 Information Security Incident Management. *Reporting and managing security events, weaknesses, and improvements.*

A.13 Information Security Incident Management		
A.13.1	Reporting information security events and weaknesses	Objective. To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
A.13.1.1	Reporting information security events	Control. Information security events shall be reported through appropriate management channels as quickly as possible.
A.13.1.2	Reporting security weaknesses	Control. All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
A.13.2	Management of information security incidents and improvements	Objective. To ensure a consistent and effective approach is applied to the management of information security incidents.

A.13.2.1	Responsibilities and procedures	Control. Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A.13.2.2	Learning from information security incidents	Control. There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
A.13.2.3	Collection of evidence	Control. Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Table 26: A.14 Business Continuity Management. Mitigating the risk of major failures and planning for timely resumption.

A.14 Business Continuity Management		
A.14.1	Information security aspects of business continuity management	Objective. To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
A.14.1.1	Including information security in the business continuity management process	Control. A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
A.14.1.2	Business continuity and risk assessment	Control. Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
A.14.1.3	Developing and implementing continuity plans including information security	Control. Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
A.14.1.4	Business continuity planning framework	Control. A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
A.14.1.5	Testing, maintaining and reassessing business continuity plans	Control. Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

Table 27: A.15 Compliance. Conforming to legal requirements, organizational security policies and standards and minimizing the performance impact of implementing audit controls.

A.15 Compliance		
A.15.1	Compliance with legal requirements	Objective. To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
A.15.1.1	Identification of applicable legislation	Control. All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
A.15.1.2	Intellectual property rights (IPR)	Control. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on

		the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
A.15.1.3	Protection of organizational records	Control. Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
A.15.1.4	Data protection and privacy of personal information	Control. Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
A.15.1.5	Prevention of misuse of information processing facilities	Control. Users shall be deterred from using information processing facilities for unauthorized purposes.
A.15.1.6	Regulation of cryptographic controls	Control. Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2	Compliance with security policies and standards, and technical compliance	Objective. To ensure compliance of systems with organizational security policies and standards.
A.15.2.1	Compliance with security policies and standards	Control. Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
A.15.2.2	Technical compliance checking	Control. Information systems shall be regularly checked for compliance with security implementation standards.
A.15.3	Information systems audit considerations	Objective. To maximize the effectiveness of and to minimize interference to/from the information systems audit process.
A.15.3.1	Information systems audit controls	Control. Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
A.15.3.2	Protection of information systems audit tools	Control. Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

NIST SP 800-61 Computer Security Incident Handling Guide

Our proposed CSPs have similar approaches to their incident response procedures—based upon guidance applicable to FedRAMP and described in NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*.

NIST SP 800-61 defines a *computer security incident* as a “violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices” and acknowledges that such incidents “frequently compromise personal and business data”, and that it is “critical to respond quickly and effectively when security breaches occur.”

NIST SP 800-61 presents a case for businesses to have in place a policy, plan, and procedures related to incident response, with a particular emphasis on outside parties such as law enforcement, media, customers, vendors, and other constituents. It describes 4 phases of handling an incident in detail—preparation (and prevention), detection and analysis, containment, eradication and recovery, and post-incident activity. The NIST guide concludes with best practices for coordinating and sharing information.

Table 28 below summarizes the recommendations found in NIST SP 800-61 as it is applicable to FedRAMP authorization.

Table 28: NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.
Recommendations of the National Institute of Standards and Technology.

Section	Recommendations
Organizing a Computer Security Incident Handling Capability	- Establish a formal incident response capability - Create an incident response policy - Develop an incident response plan based on the incident response policy - Develop incident response procedures - Establish policies and procedures regarding incident-related information sharing - Provide pertinent information on incidents to the appropriate organization - Consider the relevant factors when selecting an incident response team model - Select people with appropriate skills for the incident response team - Identify other groups within the organization that may need to participate in incident handling - Determine which services the team should offer
Handling an Incident	- Acquire tools and resources that may be of value during incident handling - Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure - Identify precursors and indicators through alerts generated by several types of security software - Establish mechanisms for outside parties to report incidents - Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems - Profile networks and systems - Understand the normal behaviors of networks, systems, and applications - Create a log retention policy - Perform event correlation - Keep all host clocks synchronized - Maintain and use a knowledge base of information - Start recording all information as soon as the team suspects that an incident has occurred - Safeguard incident data. - Prioritize handling of the incidents based on the relevant factors - Include provisions regarding incident reporting in the organization's incident response policy. - Establish strategies and procedures for containing incidents. - Follow established procedures for evidence gathering and handling. - Capture volatile data from systems as evidence. - Obtain system snapshots through full forensic disk images, not file system backups - Hold lessons learned meetings after major incidents
Coordination and Information Sharing	- Plan incident coordination with external parties before incidents occur to ensure that all parties know their roles and that effective lines of communication are established - Consult with the legal department before initiating any coordination efforts—there may be contracts or other agreements that need to be put into place before discussions occur - Perform incident information sharing throughout the incident response life cycle - Attempt to automate as much of the information sharing process as possible - Balance the benefits of information sharing with the drawbacks of sharing sensitive information - Share as much of the appropriate incident information as possible with other organizations - Organizations should consider which types of technical information should or should not be shared with various parties—there may be both security and liability reasons why an organization would not want to reveal the details of an exploited vulnerability

Requirement 8.3.2

Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

- ✓ Please see Emergent's response to Requirement 8.6.4, specifically **Table 36: Ensuring Data Confidentiality** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.

Requirement 8.3.3

Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.
- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 6.5.3 with respect to **Table 8** identifying the service models, deployment models, and risk category for each of our proposed CSPs.
- ✓ Please see Emergent's response to Requirement 6.6 with respect to the scope and variety of the solutions we have proposed to offer under this solicitation.
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
- ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Each of our proposed CSPs offer a wide variety of solutions—from familiar, yet proprietary platforms such as Microsoft and VMware to the basic building block provided by SoftLayer to the seemingly overwhelming number of options from AWS.

Leveraging the tools afforded to them, customers have control over their data and how they want it processed as they consume cloud resources. Tools such as ASW CloudFormation and Microsoft's Resource Manager are the perfect solution for spinning up user test/staging environment that would be identical to production.

Requirement 8.3.4

Offeror must describe whether or not its computer applications and Web sites are be accessible to people with disabilities, and must comply with Participating entity accessibility policies and the Americans with Disability Act, as applicable.

Applicable and up-to-date Voluntary Product Accessibility Templates (VPATs) can be found on the websites of each of our proposed CSPs:

Amazon Web Services	AWS offers provides accessibility information upon request
Microsoft Azure	VPATs for Microsoft products can be found here
VMware vCloud Air	VMware offers VPATs on their website
SoftLayer	IBM Product Accessibility Information is available upon request .

Requirement 8.3.5

Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum.

Web browsers supported by our proposed CSPs include:

Amazon Web Services	✓ Last 3 versions of Google Chrome
	✓ Last 3 versions of Mozilla Firefox
	✓ Microsoft Internet Explorer 9, 10, and 11
	✓ Microsoft Edge 12
	✓ Apple Safari 6, 7, 8, and 9
Microsoft Azure	✓ Google Chrome (latest)
	✓ Mozilla Firefox (latest)
	✓ Microsoft Internet Explorer 11
	✓ Microsoft Edge (latest)
	✓ Apple Safari (latest)
VMware vCloud Air	✓ Google Chrome 10 and later
	✓ Mozilla Firefox 3.6 and later
	✓ Microsoft Internet Explorer 8 and later
	✓ Apple Safari 4 and later
SoftLayer	✓ Google Chrome 10 and later
	✓ Mozilla Firefox 3.6 and later
	✓ Microsoft Internet Explorer 8 and later

Requirement 8.3.6

Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

- ✓ Please see Emergent's response to Requirement 8.6.4, specifically **Table 36: Ensuring Data Confidentiality** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.
- ✓ Please see Emergent's response to Requirement 8.7.1 with respect to managing the end of life activities of closing down a service.
- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

Requirement 8.4 (E) CUSTOMER SERVICE

Requirement 8.4.1

Offeror must describe how it ensures excellent customer service is provided to Purchasing Entities. Include:

- *Quality assurance measures;*
-

- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA).

Customer Service: Service Level Agreements

- ✓ Please see Emergent's response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Customer Service: Support Plans

The tables below summarize the applicable and up-to-date that can be found on the websites of each of our proposed CSPs:

Amazon Web Services [AWS Support Plans](#)

Microsoft Azure [Azure Support for Customers](#)

VMware vCloud Air [vCloud Support Offerings](#)

SoftLayer [SoftLayer Support](#)

Amazon Web Services: Support Plans

Table 29: AWS Support Plans. Customers receive basic support at no cost and have the option to increase the level of support.

AWS Support	Basic (No charge)	Developer	Business	Enterprise
Customer Service and Communities	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums
Best Practices	Access to 4 core Trusted Advisor checks	Access to 4 core Trusted Advisor checks	Access to full set of Trusted Advisor checks	Access to full set of Trusted Advisor checks
Technical Support		Business hours* access to Cloud Support Associates via email	24x7 access to Cloud Support Engineers via email, chat & phone	24x7 access to Sr. Cloud Support Engineers via email, chat & phone
Who Can Open Cases		One primary contact/ Unlimited cases	Unlimited contacts/ Unlimited cases (IAM supported)	Unlimited contacts/ Unlimited cases (IAM supported)
Case Severity/ Response Times		Normal: < 12 hours Low: < 24 hours	Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours	Critical: < 15 minutes Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours
Architecture		General guidance	Contextual guidance	Consultative review

Support			based on your use-case	and guidance based on your applications and solutions
Launch Support			Infrastructure Event Management (Available for additional fee)	Infrastructure Event Management (Included)
Programmatic Case Management			AWS Support API	AWS Support API
Third-Party Software Support			Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting
Account Assistance				Assigned Support Concierge
Proactive Guidance				Designated Technical Account Manager

AWS first-contact response times are based on the customer's chosen severity level for each case. AWS will use all reasonable efforts to provide responses within these time frames:

Table 30: AWS Support. Response times vary based on the level of support and the severity of the request.

	Critical	Urgent	High	Normal	Low
Enterprise Plan (24x7)	<= 5 minutes	<= 1 hour	<= 4 hours	<= 12 hours	<= 24 hours
Business Plan (24x7)		<= 1 hour	<= 4 hours	<= 12 hours	<= 24 hours
Developer Plan (Business hours*)				<= 12 hours	<= 24 hours

Microsoft Azure: Support Plans

Table 31: Microsoft Azure Support. All levels of support are paid-for services and have the option to increase the level of support.

Microsoft Azure Support	Developer	Standard	Professional Direct	Premier
Best for:	Non-production environment	Limited business critical dependence on Azure	Substantial dependence on Azure	Business critical, strategic dependence on Azure
Range of support	Microsoft Azure	Microsoft Azure	Microsoft Azure	All Microsoft products
Unlimited 24x7 technical support	✓	✓	✓	✓
Non-Microsoft technologies running on Azure	✓	✓	✓	✓
Advisory services	--	--	Limited advisory	Customer-specific

Support account management	--	--	Pooled	Assigned
Escalation management	--	--	✓	✓
Cloud Service Dependency Mapping	--	--	--	✓
Onsite support	--	--	--	✓
Initial response time *	< 1 business day	< 2 hours	< 1 hour	< 15 minutes
Maximum severity	C	A	A	A

VMware vCloud Air: Support Plans

Table 32: VMware vCloud Support. All levels of support are paid-for services and have the option to increase the level of support.

Feature	SaaS Production	SaaS Basic
Hours of Operation	24 Hrs/Day 7 Days/Wk 365 Days/Yr	12 Hrs/Day Mon-Fri
Length of Service	1 Year	1, 2 or 3 Years
Product Updates	Yes-SaaS Updates [1]	Yes-SaaS Updates [1]
Product Upgrades	No	No
Products Supported	Support by Product Matrix	Support by Product Matrix
Method of Access	Telephone/Web [2]	Telephone/Web [2]
Response Method	Telephone/Email	Telephone/Email
Remote Support	Yes	Yes
Access to VMware Web site	Yes, and access to product SaaS Performance Dashboard [3]	Yes, and access to product SaaS Performance Dashboard [3]
Access to VMware Discussion Forums and Knowledge Base	Yes	Yes
Max Number of Support Admins per Contract	6 [4]	4 [4]
Number of Support Requests	Unlimited	Unlimited

SoftLayer: Free Support

Support Resources

KnowledgeLayer

- ✓ Access to FAQs, how-to guides, walkthroughs, and documentation for all products and services
- ✓ Useful for all levels, from new users to experienced users

SoftLayer Development Network (SLDN)

- ✓ Reference SoftLayer API documentation
- ✓ Find API code examples and release notes
- ✓ Get tips and tricks from SoftLayer developers

SoftLayer on Social Media

- ✓ Talk cloud with cloud experts
- ✓ Stay up-to-date with the SoftLayer news
- ✓ Learn more about SoftLayer products and services

Full-service Support

Phone (866.403.7638)

- ✓ Dedicated toll-free and local phone support
- ✓ Rapid initial response, typically within seconds

Tickets

- ✓ Integrated ticket support is built into our customer portal, enabling interactive trouble shooting with a rapid initial response, typically within 20 minutes
- ✓ Intuitive user friendly interface through our customer portal providing up to date status on all open support tickets
- ✓ The permissions setting allows only specified account users to receive event notifications, perform specified functions, and access secure information.

Table 33: SoftLayer Support. Support is provided at no additional cost.

SoftLayer Support		Self-service Support	Support Resources	Full-service Support
Devices	Bare Metal/Virtual Server	✓	✓	✓
	Monitoring	✓	✓	✓
Storage	Block/File	✓	✓	✓
	Object Storage	✓	✓	✓
	Content Delivery Network	✓	✓	✓
	EVault Backup	✓	✓	✓
Network	Virtual Private Network	✓	✓	✓
	Gateway Appliances	✓	✓	✓
	Load Balancers	✓	✓	✓
	Direct Link	✓	✓	✓
Services & Security	Security Software	✓	✓	✓
	SSL Certificates	✓	✓	✓
	Domain Name Service	✓	✓	✓

Requirement 8.4.2

Offeror must describe its ability to comply with the following customer service requirements:

- a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.*
 - b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.*
 - c. Customer Service Representative will respond to inquiries within one business day.*
 - d. You must provide design services for the applicable categories.*
 - e. You must provide Installation Services for the applicable categories.*
-

Emergent's Cloud and Security Sales team is staffed with trained customer service representatives and will be responsible for responding to inquiries within one business day and held accountable to being available during the requested, or subsequently revised, working hours by phone or email to support NASPO/ValuePoint customers.

- ✓ Please see Emergent's response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs
- ✓ Please see Emergent's response to Requirement 8.4.1 with respect the support plans offered by each of our proposed CSPs
- ✓ Please see Emergent's response to Requirement 8.17.1 and 8.17.2 with respect to provisioning services.
- ✓ Please see Emergent's response to Requirement 8.21 with respect to our consulting organization.

Requirement 8.5 (E) SECURITY OF INFORMATION

Requirement 8.5.1

Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Each of our proposed CSPs subscribes to a shared responsibility model. Therefore, it is important that customers understand:

- Customers continue to own their data.
- Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
- Customers can download or delete their data whenever they like.
- Customers should consider the sensitivity of their data, and decide if and how to encrypt the data while it is in transit and at rest.

Each CSP provides customers with the ability to delete their data. However, customers retain control and ownership of their data, and it is the customer's responsibility to manage their data.

Similarly, it is the customer's responsibility to provision/deprovision resources.

More details can be found in Emergent's response to Requirement 8.7.1 and Requirement 8.11.

Requirement 8.5.2

Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Most States have a broader definition of *personal information* than what is considered the general definition:

- “An individual’s first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver’s license number or state- issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.”
- For example, Arkansas, California, Florida, Missouri, Montana, Nevada, New Hampshire, North Dakota, Oregon, Rhode Island, Virginia, Wyoming, Puerto Rico include some level of *medical information* in their definition of *personal information*.

Similarly, most states have included additional conditions under which a *breach of security* notification is triggered beyond what is considered the general condition:

- “The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information.”
- For instance, Connecticut, New Jersey, and Puerto Rico breach statues define *breach of security* to mean *unauthorized access to*.

In good faith, Emergent is committed to complying with all applicable laws related to data privacy and security. However, we respectfully decline to agree with the requirement as Emergent cannot reasonably be expected to review and determine applicability of all possible laws related to data privacy and security that may be required in subsequent Participating Addendums.

- ✓ Please also see Emergent’s response to Requirement 8.6.4, specifically **Table 36: Ensuring Data Confidentiality** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.

Requirement 5.6.4

Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

- ✓ Please see Emergent’s response to Requirement 8.6.4, specifically **Table 36: Ensuring Data Confidentiality** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service.

- ✓ Please see Emergent's response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Requirement 8.6 (E) PRIVACY AND SECURITY

Requirement 8.6.1

Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

Emergent will only offer solutions from CSPs that comply with NIST SP 800-145 and other relevant industry standards as it relates to the scope of the contemplated contract.

Requirement 8.6.2

Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Emergent's proposed CSPs are committed to adopting industry best practices, adhering to global standards, and achieving certifications in various areas to deliver its cloud services.

Amazon Web Services AWS Cloud Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs—helping customers to establish and operate in an AWS security control environment.

Microsoft Azure The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve in the future. It also makes it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft to maintain and expand its portfolio of third-party certifications. These help customers demonstrate compliance readiness to their customers, auditors, and regulators. As part of its commitment to transparency, Microsoft shares third-party verification results with its customers.

VMware vCloud Air

VMware is committed to delivering a cloud service that adopts industry best practices in order to meet a comprehensive set of international and industry specific security and compliance standards. VMware adheres to rigorous security standards and is rapidly expanding coverage for various industry-specific security and compliance measures.

VMware makes independent third-party examination and audit reports available to customers that will satisfy a wide range of customer specific compliance requirements.

SoftLayer

Because the physical and virtual controls of SoftLayer's facilities, network, and customer portal are an extension of their own, customers require access to reports and information for their own compliance needs. SoftLayer's compliance department works with independent auditors and third-party organizations to meet the industry's most stringent guidelines and makes it easy for customers to get the information they need for their own audits.

Table 34: Cloud Compliance and Security. *Our CSPs conform to global industry standards—verified by third-party audits.*

Standard, Certification, or 3rd Party Attestation	AWS	Microsoft Azure	VMware vCloud Air	SoftLayer
Content Delivery and Security Association (CDSA)	Yes	Yes		
Criminal Justice Information Services (CJIS)	Yes	Yes	Yes	
CSA STAR Consensus Assessments Initiative Questionnaire (CAIQ)	Yes	Yes	Yes	Yes
Offers EU Model Clauses	Yes	Yes		Yes
US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11	Yes	Yes		
Federal Risk and Authorization Management Program (FedRAMP)	Yes	Yes	Yes	Yes
Family Educational Rights and Privacy Act (FERPA)	Yes	Yes		
Federal Information Processing Standard (FIPS) PUB 140-2	Yes	Yes	Yes	
Federal Information Security Management Act (FISMA)	Yes	Yes	Yes	Yes
Health Insurance Portability and Accountability Act (HIPAA)	Yes	Yes	Yes	Yes
ISO 9001	Yes			
ISO/IEC 27001	Yes	Yes	Yes	Yes
ISO/IEC 27017	Yes			Yes
ISO/IEC 27018	Yes			Yes
International Traffic in Arms Regulations (ITAR)	Yes			
Multi-Level Protection Scheme (MLPS)	Yes	Yes	Yes	Yes
Payment Card Industry (PCI) Data Security Standards (DSS)	Yes	Yes		Yes

UK G-Cloud 6	Yes	Yes	Yes	Yes
Service Organization Control (SOC)				
SOC 1 (SSAE16)	Type 2	Type 2	Type 2	Type 2
SOC 2	Type 2	Type 2	Type 2	Type 2
SOC 3	Yes	Yes	Yes	Yes

Requirement 8.6.3

Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

In the traditional datacenter model, the IT organization controls networked systems, including physical access to networking equipment. In the cloud service model, the responsibilities for network protection and management are shared between the CSP and the customer. Customers do not have physical access, but they implement the logical equivalent within their cloud environment.

Our proposed CSPs are well known for protecting trust and for investing in their security infrastructures. These include multiple levels of built-in security and multi-layer security architecture options customers can superimpose on top of their cloud environment. Plus these security measures meet many of the standards set by governments and the industry such as the US Department of Defense (DoD) 5220.22-m standards, the NIST 800-53 framework, and compliance with FedRAMP HIPAA, FISMA, and SOC 2 Type 2.

Table 35 below describes the policies and procedures each of our proposed CSPs has in place to secure data and applications from threats outside the service center as well as other customer co-located within the same service center.

Table 35: Securing Data and Applications from Threats. AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each have different approaches to securing data and applications from threats inside and outside their service centers.

CSP	Security Practices to Secure Data and Applications
Amazon Web Services	Detect unusual or unauthorized activities and conditions at ingress and egress communication points. AWS tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity. Systems instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel. Available documentation to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a conferencing system is used which supports communication and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. Post-mortems are convened after any significant operational issue, regardless of external impact, and Cause of Error (COE) documents are drafted so the root cause is captured and preventative actions are taken in the future. While customers can implement further protection, the AWS network provides significant protection against traditional network security issues such as:

	• Distributed Denial Of Service (DDoS) Attacks. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity. • Man in the Middle (MITM) Attacks. All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. • IP Spoofing. Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own. • Port Scanning. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by customers. However, customers are responsible for using appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. • Packet sniffing by other tenants. It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance—even if two virtual instances are owned by the same customer located on the same physical host. While Amazon EC2 does provide ample protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice customers should encrypt sensitive traffic.
Microsoft Azure	Network Isolation. Azure is a multitenant service, meaning that multiple customers' deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data. Virtual Networks. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks. VPN and Express Route. Microsoft enables connections from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs. For even better performance, customers may use ExpressRoute, a private fiber link into Azure data centers that keeps their traffic off the Internet. Encrypting Communications. Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises data centers.
VMware vCloud Air	Network Perimeter Protection. The vCloud Air architecture is built to protect network entry points for its tenants assigned to customers. • Highly-available edge gateways and segmented network components are dedicated and configured by each tenant to protect the perimeter of their environment. • VMware protects the control and management plane from attack by employing firewalls that can be configured with customer specific policies, intrusion detection, network segmentation, as well as threat mitigation and zero-day anomaly detection and mitigation for all VMware-managed infrastructure components. • Customers are responsible for the security of the networks over which they have administrative level control, including, but not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, secure VPN access, etc. Security Tools. vCloud Network and Security Edge Gateways provide Load Balancing, VPN, Firewall and NAT services, but customers may augment this technology with third-party network and security solutions, such as those found in the VMware Solution Exchange, and agent-based security and monitoring tools to ensure service stability and integrity. • Third-party networking or security utilities deployed within vCloud Air require customer validation to ensure their security objectives are met • Virtual appliances housed within the VMware Solution Exchange are supported, but not maintained,

	by VMware. vCloud Air operates co-location facilities allows customers to co-locate in the same physical data center and deploy their preferred security tools to maintain the exact same set of controls, security tools and posture that exist in their private data centers.
SoftLayer	Secure connectivity, authentication, access control, and audit capabilities for IT administrators and users. This includes VPNs, multifactor authentication, audit control logs, API keys, and other fine-grained access control allowing customers to securely access work data and connect to the application via HTTPS using SSL certificates. Enforce stringent data security measures—leaving data where customers place it, and never transferring it. Data cannot be shifted across borders, and data-at-rest and data-in-transit must be encrypted. SoftLayer offers encryption solutions such as CloudLink Secure VM, IBM Cloud Data Encryption Services (ICDES), and ProtectV and Virtual KeySecure from SafeNet to ensure sensitive data-at-rest is not stored in clear text and that the customer maintains complete control of encryption keys. Ensure multi-layered security for network zone segmentation. Because customers need confidence that their network is securely partitioned, SoftLayer provides native and vendor solutions such as SoftLayer VLANs, Vyatta Gateway, Fortigate firewall, and Citrix Netscaler that allow administrators to securely partition a network, creating segmentation according to organizational needs and providing the routing and filtering needed to isolate users, workloads, and domains. Enforce host security using anti-virus software, host intrusion prevention systems, and other solutions. By applying best-of-breed third-party solutions such as Nessus Vulnerability Scanner, McAfee Antivirus, and McAfee Host Intrusion Protection, administrators have the means to ensure that infrastructure is protected from malware and other host attacks—enhancing both system availability and performance. Enable customers to define and enforce security policies for hybrid cloud environments—and audit any policy changes. SoftLayer manages overall policies for the combined public-private environment using IBM solutions like QRadar, Hosted Security Event and Log Management Service, and xForce Threat Analysis Service. Customers may use solutions from vendors like CloudPassage, Sumo Logic, and ObservelT to automatically define policies around firewall rules, file integrity, security configuration, and access control—and to audit adherence to such policies.

Requirement 8.6.4

Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

SOC 1 Type 2 audit report attests to the design and operating effectiveness of controls. The SOC 2 Type 2 audits include a further examination controls related to security, availability, and confidentiality. Each of our proposed CSPs is audited annually to ensure compliance with the standards set by governments and the industry as noted in the previous section.

Table 36 below describes the policies and procedures our proposed CSPs have in place to ensure access to customer data is only to provide the service, including purposes compatible with providing the service; and that it does not use customer data for advertising or similar commercial purposes.

Table 36: Ensuring Data Confidentiality. AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer have data confidentiality standards and practices restricting access to customer data.

CSP	Data Confidentiality Practices
Amazon Web	Access. Customers manage access to their customer content and AWS services and resources. AWS provides customers an advanced set of access, encryption, and logging features. AWS does not access

Services	or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to customers and their end users. Storage. Customers choose the region(s) in which their customer content will be stored. AWS will not move or replicate customer content outside of the customer's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to customers and their end users. Security. Customers choose how their customer content is secured. AWS offers customers strong encryption for customer content in transit or at rest, and provides customers with the option to manage their own encryption keys. Disclosure of customer content. AWS does not disclose customer content unless required to do so to comply with the law or a valid and binding order of a governmental or regulatory body. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure. Security Assurance. AWS has developed a security assurance program using global privacy and data protection best practices in order to helping customers establish, operate and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.
Microsoft Azure	Customer data is only accessed when necessary to support the customer's use of Azure. This may include troubleshooting aimed at preventing, detecting, or repairing problems affecting the operation of Azure and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is controlled and logged. Strong authentication, including the use of multifactor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. Microsoft will not disclose Azure customer data to law enforcement except as a customer directs or where required by law. When governments make a lawful demand for Azure customer data, Microsoft strives to be principled, limited in what they disclose, and committed to transparency. In its commitment to transparency, Microsoft regularly publishes a Law Enforcement Requests Report that discloses the scope and number of requests they receive.
VMware vCloud Air	Customers are solely responsible for their own content. Customer access is restricted to that content and data. Customers do not have the ability to view content from any other customer using the service, and the service is architected from the ground up with this principle in mind. VMware accesses and uses this content only as necessary to provide the Service Offering (which may be done with the assistance of a affiliates, service providers and contractors), perform or enforce contractual obligations, or comply with applicable law.
SoftLayer	On occasion, employees of SoftLayer that are located in the U.S. may have temporary access to customer content in connection with providing maintenance or support services. This access will only be accomplished by way of the customer's explicit permission and instructions and only for so long as the employee is providing services to the customer. As a processor, SoftLayer will not access the customer content for any purpose beyond providing the customer with support as described above, and will not disclose it to any person or entity.

Requirement 8.6.5

Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to data security, integrity, and other controls.

- ✓ Please see Emergent's response to Requirement 8.6.2, specifically **Table 34: Cloud Compliance and Security** that contains a detailed list of third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to data security, integrity, and other controls for each CSP we are proposing.

Requirement 8.6.6

Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Table 37: sdds

CSP	Logging Features
Amazon Web Services	Available as an optional service, AWS CloudTrail provides visibility into user activity by recording API calls made on a customer account. CloudTrail records important information about each API call, including the name of the API, the identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service. This information helps track changes made to AWS resources and to troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.
Microsoft Azure	Available as an optional service, Log Analytics is the log analysis service and core functionality in Microsoft's Operations Management Suite (OMS). It helps IT administrators to gain insight across on-premises and cloud environments and interact with real-time and historical machine data to develop custom insights. Log Analytics provides proactive operational data analysis through the delivery of solutions. Administrators can add solutions using the integrated gallery and consisting of pre-built rules and algorithms that perform initial analysis for critical scenarios like capacity planning, configuration intelligence and change tracking. Use cases include: • Search and investigate by typing key words, values and fields to uncover valuable and actionable insights throughout the infrastructure then export desired data • Create custom dashboards by choosing different chart visuals and setting thresholds • Plan for capacity to get deep visibility into the data center capacity, investigate "what-if" scenarios, identify stale and over allocated virtual machines, and plan future compute and storage needs • Investigate system update status and identify missing system updates across all servers whether they're running in the data center or in a public cloud. • Log analytics helps to easily identify operational issues caused by software changes that occur in your environment • Detect security breaches by enabling an efficient, scalable, and secure way to collect and store security records. The search capabilities provide the ability to answer the question of who did what, when and on which devices • Collect security logs which helps security analysts and system admins mine large distributed sets of security data in order to detect suspicious activities and potential security breaches • Collect network and performance data using wire data combined with other data to help identify network activity for other processes and users
VMware vCloud Air	vCloud Director provides logging information for each cloud cell in the system. You can view the logs to monitor your cells and to troubleshoot issues. Data collected includes: • Console output from the vCloud Director cell. • Cell diagnostics log. This file is empty unless diagnostics logging is enabled in the local logging configuration. • Informational log messages from the cell. This log also shows warnings or errors encountered by the cell. • Debug-level log messages from the cell. • Informational log messages from the cell watchdog. It records when the cell crashes, is restarted, etc.
SoftLayer	SoftLayer event logs are always active and protected from unauthorized access. Significant events (including login attempts, privilege escalations) are logged and analyzed. Appropriate information is collected in SoftLayer platform logs that allow for analysis, identification and audit of the platform. SoftLayer regularly monitors and analyzes security logs generated from platform componentry for irregular suspicious activities. Logged alerts are handled in a timely manner and, if applicable information is

	communicated to the client via the standard incident response and support mechanisms. The SoftLayer platform allows customers to implement "least privileged" for staff access. Tasks and duties specific to managing systems are segregated in order to reduce the possibilities of unauthorized access—whether involuntary or deliberate. SoftLayer only provides security logs to customers who have provisioned and configured a network and application level firewalls that protect the subscribed resources. SoftLayer provides detailed information through the SoftLayer portal and is available for download by customer through the API for events such as user authentication (including successful, unsuccessful and password change requests). All activities undertaken by SoftLayer in response to customer request (e.g. replace a hard drive) are recorded in a service ticket that can be viewed in portal or downloaded via API. This provides customer with detailed information on the management of their environment.

Requirement 8.6.7

Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Each of our proposed CSPs provide IAM solutions that, when properly implemented, satisfy their customers' mission-critical needs to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.

- ✓ Please see Emergent's response to Requirement 8.16.1, specifically **Table 42: Identity and Access Management** describes how AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer provide IAM capabilities.

Requirement 8.6.8

Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

- ✓ Please see Emergent's response to Requirement 8.3.1 with respect to how each of our CSPs handle security incidents compliant with ISO/IEC 27001 and NIST SP 800-61.

Requirement 8.6.9

Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Physical Security

Our proposed CSPs physical infrastructure is geographically distributed across the globe and designed to operate 24x7x365. Various measures are employed to help protect operations from power failure, physical intrusion, and network outages. Datacenters comply with industry standards, such as ISO/IEC 27001, SOC 1 Type 2 and SOC 2 Type 2, for physical security and availability and are managed, monitored, and administered by CSP operations personnel. Features include:

- **Perimeter.** Security staff, badged access, barriers, facility setback requirements, and fencing
- **Buildings.** Alarms, Security operations center, seismic bracing, and security cameras

- **Computer Room.** Cameras, days of backup power, and two-factor access control: biometric and card readers

Virtual Control

Each of our proposed CSPs allows customers to provision a logically isolated section of their cloud in a turn-key fashion to create virtual environments with minimal configuration. The infrastructure is dedicated to only the customer's instances whereby they have complete control over their virtual networking environment, including selection of IP address range, creation of subnets, and configuration of route tables and network gateways.

Requirement 8.6.10

Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS)

Each of our proposed CSPs share similar views with respect to developing and deploying secure, high performing, and cost efficient solutions in the cloud. And while migrating applications to the cloud—even without significant changes (an approach known as “lift and shift”)—realizes the benefits of a secured and cost-efficient infrastructure, engineers must evolve their architectures to take advantage of the elasticity and agility of the cloud.

With cloud computing, IT assets become programmable resources. Organizations can access as much or as little as they need and dynamically scale to meet actual demand, while only paying for what they use. In the cloud, servers, databases, storage, and higher-level application components can be instantiated within seconds. Developers can treat these as temporary and disposable resources, free from the inflexibility and constraints of a fixed and finite IT infrastructure. This resets legacy approaches to change management, testing, reliability, and capacity planning.

Taking advantage of global infrastructure, applications are deployed geographically to best meet requirements (e.g., proximity to end users, compliance, or data residency constraints, cost, etc.) and achieve high availability and fault tolerance. Combined with virtually unlimited capacity, future expansion of IT environments is not constrained.

Access to a broad set of high managed storage, database, analytics, application, and deployment services reduces dependency on in-house specialized skills and accelerates solution development at the same time lowering operational complexity and cost. Built-in security features and controls conforming to industry standards and regulatory requirements help achieve higher levels of data protection and compliance. With the ability to spin up temporary environments, security testing can now become part of a continuous delivery pipeline.

Elements of a security technical reference architecture shared by each of our proposed CSPs include:

Access Monitoring and Logging	Data Protection (at Rest & in Transit)	Notification of Lawful Requests for Information
Anti-Virus/Anti-Malware	DDoS Protection	Open APIs
Availability	Employee Qualifications	Patch/Update Management
Breach Notification/Incident Response	Encryption	Physical Security
Business Continuity/Backup/Restore	End Point Security	Privacy Considerations/ Restricted Access
Contractual Commitments	Gateways	Protecting Data at Rest
Customer Control of Data	Industry Standards	Protecting Data in Transit
Data Destruction	Intrusion Protection/Detection	Regulatory Compliance
Data Isolation	Management Portals and Tools	SSL Certificates
Data Protection	Monitoring and Logging	Transparency
Data Redundancy	Multi-Factor Authentication	

Requirement 8.7 (E) MIGRATION AND REDEPLOYMENT PLAN

Requirement 8.7.1

Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Each of our proposed CSPs have similar procedures and provide guidance to customers choosing to close an account or cancel a device:

1. Cancellations may occur immediately (hourly instances) or at the billing anniversary date (monthly/annual subscriptions). Due to the number of offerings, customers are advised to understand the termination provisions in the service contract.
2. To ensure no other accounts will have access to customer data, hard drives are decommissioned compliant with DOD 5220.22-M or NIST 800-88. This process is monitored and logged to provide an auditable history of any drive. Once complete the drive is ready to be redeployed to a new customer.
3. Customer responsibilities include, but may not be limited to:
 - 3.a. Backing up any applications and data they wish to retain prior to closing and account or cancelling a device.
 - 3.b. Deleting existing applications and associated data to avoid any future consumption charges.
 - 3.c. Any charges accrued during the billing cycle.
 - 3.d. Reviewing the terms and conditions of the service, especially with respect to customer data, and understanding what sections survive the termination of an agreement.

- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

Requirement 8.7.2

Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

- ✓ Please see Emergent's response to Requirement 8.6.4, specifically **Table 36: Ensuring Data Confidentiality** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.
- ✓ Please see Emergent's response to Requirement 8.7.1 with respect to managing the end of life activities of closing down a service.
- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

Requirement 8.8 (E) SERVICE OR DATA RECOVERY

Requirement 8.8.1

Describe how you would respond to the following situations; include any contingency plan or policy.

- a. Extended downtime.
- b. Suffers an unrecoverable loss of data.
- c. Offeror experiences a system failure.
- d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
- e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

- ✓ Please see Emergent's response to Requirement 8.3.1 with respect to how each of our CSPs handle security incidents compliant with ISO/IEC 27001 and NIST SP 800-61.

Requirement 8.8.2

Describe your methodologies for the following backup and restore services:

- a. Method of data backups
- b. Method of server image backups
- c. Digital location of backup storage (secondary storage, tape, etc.)
- d. Alternate data center strategies for primary data centers within the continental United States.

CSP	Data Confidentiality Practices
Amazon Web Services	Amazon Simple Storage Service (S3). Provides developers and IT teams with secure, durable, and highly-scalable cloud storage solution. Configurable through a simple web service interface customers pay only for the storage they actually use and there is no minimum fee and no setup cost. Amazon Glacier. Amazon Glacier is a secure, durable, and extremely low-cost cloud storage service for data archiving and long-term backup.

	Storage Gateway. The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. The service allows customers to securely store data in the AWS cloud for scalable and cost-effective storage. EC2. Regularly back up instances using Amazon EBS snapshots or a backup tool. Customers can prepare to handle failover by manually attaching a network interface or Elastic IP address to a replacement instance or leverage an automated solution, such as Auto Scaling.
Microsoft Azure	Azure Backup. Simple and reliable cloud integrated backup as a service: • Unified solution to protect data on-premises and in the cloud • 99.9% availability guaranteed • Reliable offsite backup target • Efficient incremental backups • Secure—data is encrypted in transit and at rest • Geo-replicated backup store Site Recovery. "Recovery as a Service" • Automated protection and replication of virtual machines • Remote health monitoring • Customizable recovery plans • No-impact recovery plan testing • Orchestrated recovery when needed • Replication to—and recovery in—Azure
VMware vCloud Air	VMware vCloud Air Disaster Recovery is a recovery-as-a-service (RaaS) solution that introduces native cloud-based disaster recovery capabilities for VMware vSphere virtual environments. Built on VMware's hypervisor-based replication engine, vSphere Replication, vCloud Air Disaster Recovery includes: • Self-service disaster recovery protection for virtual machines • Recovery point objectives (RPO) from 15 minutes to 24 hours • Readily facilitates failover, failback and planned migration as needed • Retention of multiple recovery points. up to 24 point-in-time instances • Elastic cloud compute and storage capacity • Support for offline data seeding • Private leased line network option Flexible failover testing
SoftLayer	EVault Backup. Simple graphical user interface initiates all backups and restores, and configures all backup and automation options. Administrators can set backups to follow an hourly, daily, weekly or custom schedule, and to target full systems, specific directories or even individual files. Individual software agents are available that enable EVault to target more specific data in Exchange, SQLServer, Sharepoint, MSClusters and Oracle servers. Idera Server Backup. Provides high-performance disk-to-disk server backup featuring a central management and data repository. This protects data at block level, and its unique disk blocks on the server are stored only once across all recovery points, increasing storage efficiency. Tape back up is not available on SoftLayer.

Requirement 8.9 (E) DATA PROTECTION

Requirement 8.9.1

Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

Each of our proposed CSPs provide standard encryption technologies and options to protect sensitive data while in transit or at rest. While AWS and Microsoft offer proprietary solutions tightly integrated into their services, all CSPs support third-party solutions available at additional costs from their respective marketplaces.

Table 38: Encryption Technologies and Options. *AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer offer different encryption technologies and options to protect sensitive data while in or at rest.*

CSP	Encryption Technologies and Options
Amazon Web Services	AWS Key Management Service (KMS) is a managed service that makes it easy for customers to create and control the encryption keys used to encrypt their data, and uses Hardware Security Modules (HSMs) to protect the security of their keys. AWS Key Management Service is integrated with several other AWS services to help customers protect their data with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide customers with logs of all key usage to help meet their regulatory and compliance needs. • Centralized Key Management. AWS Key Management Service provides customers with centralized control of encryption keys. KMS presents a single view into all of the key usage in the organization. Customers can easily create keys, implement key rotation, create usage policies, and enable logging from the AWS Management Console, or by using the API. • Integrated with AWS services. AWS Key Management Service is integrated with several other AWS services to make it easy to encrypt the data customers store with these services using keys that they manage. • Encryption for all applications. AWS Key Management Service makes it easy to manage encryption keys used to encrypt data stored by applications regardless of where customers store it. KMS provides an SDK for programmatic integration of encryption and key management into applications. • Built-in Auditing. AWS Key Management Service works with AWS CloudTrail to provide customers with logs of API calls made to or by KMS. These logs help customers meet compliance and regulatory requirements by providing details of when keys were accessed and who accessed them. • Fully Managed. AWS Key Management Service is a fully managed service, so customers can focus on the encryption needs of applications while AWS handles availability, physical security, and hardware maintenance of the underlying infrastructure. • Low-cost. There is no charge for the storage of default keys in a customer account. Customers pay only for additional master keys that they create and their key usage. • Secure. AWS Key Management Service provides customers a secure location to store and use encryption keys, using hardened systems where unencrypted keys are only used in memory. KMS keys are never transmitted outside of the AWS regions in which they were created. • Compliance. Security and quality controls in AWS KMS have been validated and certified by a number of compliance schemes.
Microsoft Azure	Windows VMs can be encrypted using the same native BitLocker Drive Encryption many enterprise customers already use to protect data stored on their on-premises Windows-based systems. Customers leveraging Linux VMs in Azure can protect them using DM-Crypt technology with a passphrase they provide. The BitLocker encryption keys or Linux DM-Crypt passphrases that are used to encrypt and decrypt the VM drives are stored in Azure Key Vault which provides protection for the keys via FIPS 140-2 Level 2

	validated hardware security modules (HSMs).
VMware vCloud Air	Available through the vCloud Air Marketplace: HyTrust DataControl. Provides encryption and key management designed specifically to address the unique requirements of private, hybrid and public clouds including vCloud Air. It keeps data on virtual machines secure through the entire lifecycle—from deployment and migration through sanctioned decommission. HyTrust also offers strong and easy-to-deploy key management, ensuring that regardless of where data resides—whether in private or public clouds—organizations always retain control over their data. DataControl can be leveraged instantly to support mandates such as PCI DSS, HIPAA/HITECH, CJIS, FedRAMP, and Data Sovereignty/Data Residency. CloudLink SecureVM. Tightly integrated with the VMware tools and platforms, it provides pre-boot authorization, image integrity validation and encrypts boot volume and data volumes with a centralized management approach that allows IT departments to have full control over data security in the cloud. SecureVM unlocks native Windows Bitlocker and Linux OS encryption features with a centralized management approach. This gives customers visibility and control over when and where virtual machines are run and accessed, while retaining full control of encryption keys.
SoftLayer	Customers choose how their customer content is secured. SoftLayer offers encryption solutions such as CloudLink Secure VM, IBM Cloud Data Encryption Services (ICDES), and ProtectV and Virtual KeySecure from SafeNet to ensure sensitive data-at-rest is not stored in clear text and that the customer maintains complete control of encryption keys.

Requirement 8.9.2

Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

HIPAA regulations require that covered entities and their business associates—in this case, our proposed CSPs when providing cloud services to covered entities—enter into contracts to ensure that those business associates will adequately safeguard protected health information (PHI). Business Associate Agreements (BAAs), clarify and limit how the business associate can handle PHI, and set forth each party's adherence to the security and privacy provisions set forth in HIPAA and the HITECH Act. Once a BAA is in place, covered entities can use the CSPs' cloud services to process and store PHI.

Currently there is no HIPAA or HITECH Act compliance certification for cloud service providers. Cloud services covered under the BAA are typically included through the audits conducted by accredited independent auditors for ISO/IEC 27001 certification and covered by the FedRAMP assessments.

Requirement 8.9.3

Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

- ✓ Please see Emergent's response to Requirement 8.6.4, specifically **Table 36: Ensuring Data Confidentiality** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.

Requirement 8.10 (E) SERVICE LEVEL AGREEMENTS

Requirement 8.10.1

Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Cloud computing affords consumers the ability to unilaterally and automatically provision computing capabilities and broad networks access. Cloud computing is achievable primarily because resources are pooled to serve multiple consumers—elastically provisioned and released and automatically controlled and optimized. Customizing SLAs for potentially millions of customers is simply not financially feasible.

In such cases where potential scale may be realized, some CSPs may be willing to negotiate SLAs. For instance, FedRAMP and G-Cloud are essentially cloud services with additional SLAs. In any event, hotly debated issues will always include indemnification, limitation of liability, breach notification, use of third-party service providers, and termination clauses.

However, Emergent is does not have blanket authority to negotiate SLAs on behalf of the CSPs we represent.

Requirement 8.10.2

Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

- ✓ Please see Emergent's response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Requirement 8.11 (E) DATA DISPOSAL

Specify your data disposal procedures and policies and destruction confirmation process.

Each of our proposed CSPs has data disposal procedures and policies that comply with DOD 5220.22-M or NIST 800-88.

NIST 800-88 provides a decision flow, seen in **Figure 2** below, used by organizations to assist them in making sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media. The decision process is based on the confidentiality of the information, not the type of media. Once organizations decide what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.

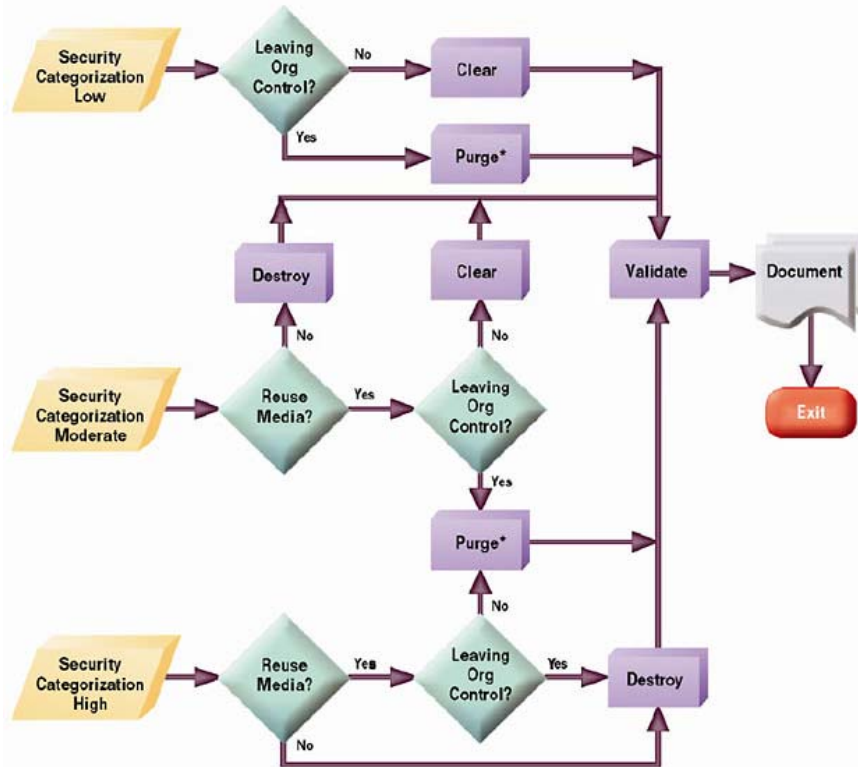


Figure 2: Sanitization and Disposition Decision Flow.

Requirement 8.12 (E) PERFORMANCE MEASURES AND REPORTING

Requirement 8.12.1

Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Table 39: Performance Measures and Reporting. While each of our proposed CSPs guarantees different levels of “uptime”, they all exceed 99.9%.

CSP	Reliability and Uptime
Amazon Web Services	All AWS SLAs offer 99.9% or greater “availability”, subject to the applicable metric (availability, send/receive, connectivity)
Microsoft Azure	All Microsoft SLAs offer 99.9% or greater “availability”, subject to the applicable metric (availability, send/receive, connectivity)
VMware vCloud Air	All VMware SLAs offer 99.9% or greater “availability, except for Object Storage. Object Storage may be purchased as “Durable Reduced Availability” or “Nearline Storage” consequently, the commitment to “availability” is 99.0% or greater.
SoftLayer	SoftLayer uses “reasonable efforts to provide a service level of 100%” for its services.

Although the formulas used by each CSP to determine “availability” differ—and may not seem to equal the percentages pledged—the simplest and most economical way of mitigating availability risks is to use more than one region.

Requirement 8.12.2

Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

- ✓ Please see Emergent’s response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Requirement 8.12.3

Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

- ✓ Please see Emergent’s response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Requirement 8.12.4

Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

- ✓ Please see Emergent’s response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Requirement 8.12.6

Describe the firm’s procedures and schedules for any planned downtime.

- ✓ Please see Emergent’s response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Requirement 8.12.7

Describe the consequences/SLA remedies if disaster recovery metrics are not met.

- ✓ Please see Emergent’s response to Requirement 5.5.4 with respect to the where the applicable and up-to-date SLAs may be found for each of our proposed CSPs

Requirement 8.12.8

Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

Table 40: Performance Measures and Reporting. *Each of our propose CSPs offer views with respect to their service performance and status.*

CSP	Service Performance and Status
Amazon Web Services	AWS service status: http://status.aws.amazon.com
Microsoft Azure	Azure service status: https://azure.microsoft.com/en-us/status/
VMware vCloud Air	vCloud status is available via vCloud Director.
SoftLayer	SoftLayer maintenance notifications: https://status.softlayer.com SoftLayer network speed test: http://speedtest.dal05.softlayer.com/speedtest/

Requirement 8.12.9

Ability to print historical, statistical, and usage reports locally.

Historical, statistical, and usage reports are configurable and available in each of our proposed CSPs' customer account management portals/consoles. However, customers are responsible for paper, ink/toner, and the process of printing the reports.

Requirement 8.12.10

Offeror must describe whether or not its on-demand deployment is supported 24x365.

All paid-for on-demand deployments are supported 24x365. Free versions or limited trials may be subject to alternative terms and conditions, including support.

Requirement 8.12.11

Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

Customers may scale-up or scale-down all paid-for on-demand services 24x365. Free versions or limited trials may be subject to alternative terms and conditions, including support.

Requirement 8.13 (E) CLOUD SECURITY ALLIANCE

Describe your level disclosure of compliance with CSA Star Registry for each Cloud solutions offered.

a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.5

✓ Please see Emergent's response to Requirement 5.5.3.

b. Completion of Exhibits 1 and 2 to Attachment B.

✓ Please see Emergent's response to Requirement 5.5.3.

c. Completion of a CSA STAR Attestation, Certification, or Assessment.

✓ Please see Emergent's response to Requirement 6.4.2, specifically **Table 6** that contains the level of disclosure with CSA STAR.

d. Completion CSA STAR Continuous Monitoring.

Per the CSA website, CSA Level 3 Continuous Monitoring is still under development. Each of our proposed CSPs has implemented and documented a Continuous Monitoring Plan that defines their approach to conducting continuous monitoring with its authorizing officials within the FedRAMP Security Assessment Framework.

Requirement 8.14 (E) SERVICE PROVISIONING

Requirement 8.14.1

Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

Requirement 8.14.2

Describe in detail the standard lead-time for provisioning your Solutions.

- ✓ Please see Emergent's response to Requirement 8.17.1 and 8.17.2 with respect to provisioning services.

Requirement 8.15 (E) BACK UP AND DISASTER PLAN

Requirement 8.15.2 and 8.15.3

Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Applicable and up-to-date information can be found on the websites of each of our proposed CSPs:

Amazon Web Services	AWS Service Terms EU Data Protection
Microsoft Azure	Microsoft Online Subscription Agreement
VMware vCloud Air	vCloud Air Service Description
SoftLayer	SoftLayer Master Services Agreement

Requirement 8.15.4

Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

Each of our proposed CSPs provide multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

However, customers own the responsibility and management of most business continuity services, whether offered as additional “all-in-one” services such as VMware’s Disaster Recovery as a Service or Microsoft’s Site Recovery or building capability through individual service offerings offered by AWS and SoftLayer to meet a customer’s unique “requirement-driven” solution.

Table 41: Multiple Data Center Support. AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each support multiple data centers located within the United States.

CSP	Multiple Data Center Support
Amazon Web Services	The AWS Cloud infrastructure is built around Regions and Availability Zones. A Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant and scalable than would be possible from a single data center. The AWS Cloud operates 33 Availability Zones within 12 geographic Regions around the world. • High Availability Through Multiple Availability Zones. Unlike virtually every other technology infrastructure provider, each AWS Region has multiple Availability Zones and data centers. Availability Zones are connected to each other with fast, private fiber-optic networking, enabling customers to easily architect applications that automatically fail-over between Availability Zones without interruption. • Improving Continuity With Replication Between Regions. In addition to replicating applications and data across multiple data centers in the same Region using Availability Zones, customers can also choose to increase redundancy and fault tolerance further by replicating data between geographic Regions. Customers can do so using both private, high speed networking and public internet connections to provide an additional layer of business continuity, or to provide low latency access across the globe. • Meeting Compliance and Data Residency Requirements. Customers retain complete control and ownership over the region in which their data is physically located, making it easy to meet regional compliance and data residency requirements. The AWS products and services that are available in each region are listed at: http://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/
Microsoft Azure	Microsoft Azure customers control the location of their data over an ever-expanding network of data centers across the globe. Most Azure services permit customers to specify the particular geography where their customer data will be stored. Data may be replicated within a selected geographic area for redundancy, but will not be replicated outside it for redundancy. The Microsoft Azure products and services that are available in each region are listed at: https://azure.microsoft.com/en-us/regions/#services
VMware vCloud Air	Dedicated Cloud. A dedicated single- tenant, physically isolated cloud IaaS that provides customers: • A broad set of capabilities among the compute services in vCloud Air • A service for migrating existing large production workloads, hosting Test/Dev environments, and developing new applications Direct Connect. A dedicated, high-throughput networking link that connects remote data centers and those in the same colocation facility to an instance in vCloud Air. Available for Dedicated, Disaster Recovery, and Virtual Private Cloud service options, Direct Connect provides an additional connection method into vCloud Air.

SoftLayer	Every aspect of a SoftLayer data center—from location and accessibility to power density and redundancy—is designed to guarantee its security, resiliency, and efficiency. And each is staffed 24x7 with experts to troubleshoot and address the rare issues that can't be directly resolved through our automated management system. SoftLayer builds each data center to the same specifications and equips it to provide the full SoftLayer catalog of services. Each data center across North America, Europe, and Asia, is connected to the SoftLayer global private network; customers can provision cloud resources where (and when) they need them.

Requirement 8.16 (E) SOLUTION ADMINISTRATION

Requirement 8.16.1

Ability of the Purchasing Entity to fully manage identity and user accounts.

An Identity and Access Management (IAM) system initiates, captures, records and manages user identities and their related access permissions in an automated fashion to facilitate access privileges and ensure all individuals and services are properly authenticated, authorized and audited in accordance with an organization's policies.

Each of our proposed CSPs provide IAM solutions that, when properly implemented, satisfy their customers' mission-critical needs to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.

Table 42: Identity and Access Management. AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each have different approaches to providing IAM capabilities.

CSP	Identity and Access Management Capabilities
Amazon Web Services	AWS Identity and Access Management (AWS IAM) provides customers the ability to create multiple users and manage the permissions of each within the customer's AWS Account. A user is an identity (within an AWS Account) with unique security credentials that can be used to access AWS Services. AWS IAM eliminates the need to share passwords or keys, and makes it easy to enable or disable a user's access as appropriate. AWS IAM implements security best practices, such as least privilege, by granting unique credentials to every user within the customer's AWS Account and only granting permission to access the AWS services and resources required for the users to perform their jobs. AWS IAM is secure by default; new users have no access to AWS until permissions are explicitly granted. AWS IAM is also integrated with the AWS Marketplace, so that customers can control who can subscribe to the software and services offered in the Marketplace. Since subscribing to certain software in the Marketplace launches an EC2 instance to run the software, this is an important access control feature. Using AWS IAM to control access to the AWS Marketplace also enables AWS Account owners to have fine-grained control over usage and software costs. AWS IAM enables customers to minimize the use of their AWS Account credentials. Once they create AWS IAM user accounts, all interactions with AWS Services and resources should occur with AWS IAM user security credentials.
Microsoft Azure	Azure Active Directory enables a single identity management capability across on-premises, cloud, and mobile solutions. Azure Active Directory is a comprehensive identity and access management solution in the cloud—combining core directory services, advanced identity governance, security, and application access management.

	While Azure Active Directory makes it easy for developers to build policy-based identity management into their applications, Azure's Active Directory Premium offers additional features to meet the advanced identity and access needs of enterprise organizations.
VMware vCloud Air	Within a public or private vCloud environment, the mechanism for authorization and authentication is available within vCloud Director. Directory services based on Lightweight Directory Access Protocol (LDAP) and network authentication protocols such as Active Directory, OpenLDAP, or Kerberos v5 can be configured with vCloud Director. User authorization is controlled through role-based access control (RBAC) within vCloud Director. Careful consideration must be given to roles and responsibilities for managing vCloud Director, whether as a provider or as a tenant. The VMware vCloud Director Administrator's Guide contains details about permissions, roles, and settings that can be modified to fit the requirements for access control within the organization. From a provider perspective, the system administrator role should be restricted to only those individuals within the provider organization's vCloud operations team that need that level of access. For other individuals within the provider organization that require only vCloud Director organization access, other roles should be used. If possible, an LDAP group for the provider administrators should be created and imported into vCloud Director with the system administrator role applied to it. All users who require this level of access can then be managed through the LDAP system. The built-in admin account should not be used for vCloud administration, and the credentials must be stored securely. From a tenant perspective, there are predefined roles. The organization administrator is the highest level of privilege, and should be limited to those individuals within the tenant organization's vCloud operations team that require that level of access. This can be achieved with the use of LDAP groups by importing them so that vCloud Director roles can be applied to them. A variety of roles exist with vCloud Director for organizations, and if required, additional roles can be created with alternate privileges. A policy of least privilege (grant only privileges required to perform the role) should be applied to all individuals who require access to the vCloud organization, with continued use of LDAP groups to assist with managing this policy.
SoftLayer	SoftLayer offers an array of hardware and software based solutions from leading IAM providers: • Citrix NetScaler, a software-based virtual appliance offered on SoftLayer infrastructure, combines an extensive portfolio of application, network and user-layer security capabilities with a rich ecosystem of interoperable partner products. • The NetScaler ICSA-certified hybrid security model pairs Layer 7 attack signature detection with an advanced learning engine to ramp up quickly and help prevent denial-of-service attacks. As an application delivery controller (ADC), NetScaler optimizes the secure delivery of all web and enterprise business applications, cloud-based services, virtual desktops and mobile services – regardless of location and access technology. Within the Customer Portal, external, two-factor authentication may be activated to add additional protection when logging into the Portal. This additional layer of security protects the account from unverified access to ensure devices, data and account information are protected. This external authentication is available in the following forms: • Symantec Validation and ID Protection Service (VIP) is a leading cloud-based strong authentication service that can enable customer's enterprises to secure access to networks and applications while preventing access by malicious unauthorized attackers. • PhoneFactor authentication provides out-of-band authentication via phone call, SMS or mobile app. SoftLayer customers most commonly use Symantec Identify Protection as their external authentication tool, providing a dynamic security code used in addition to the username and password when accessing the Customer Portal.

Requirement 8.16.2

Ability to provide anti-virus protection, for data stores.

The term *antivirus* became popular in the 90's; today viruses are the minority when it comes to malware. Viruses are a specific type of malware designed to replicate and spread, while *malware* is used to describe a wide variety of malicious code—viruses, worms, Trojans, rootkits, botnets, and spam.

Each of our proposed CSPs provide antivirus/antimalware solutions that, when properly implemented, satisfy their customers' mission-critical needs to ensure its environments are protected from malware—be it viruses or any potentially unwanted software.

Table 43: Antivirus and Antimalware. AWS, Microsoft Azure, VMware vCloud Air, and SoftLayer each have different approaches to providing protection from viruses and malware.

CSP	Anti-Malware and Anti-Virus Capabilities
Amazon Web Services	AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO/IEC 27001 and FedRAMP. Customers are encouraged to protect their systems in the cloud as they would protect their conventional infrastructure from threats such as viruses, worms, Trojans, rootkits, botnets, and spam. The AWS Marketplace offers anti-malware and anti-virus solutions from reputable providers such as Fortinet, Trend Micro, Barracuda, CheckPoint, Symantec, and others.
Microsoft Azure	Microsoft scans Azure software components for viruses before moving to production and provides native anti-malware on all Azure virtual machines (VMs). Microsoft recommends customers install Microsoft or third-party anti-malware or anti-virus solutions on all VMs, and clean out intrusions that may have gone undetected by regularly re-imaging VMs.
VMware vCloud Air	VMware vShield Endpoint manages anti-virus and anti-malware policies for virtualized environments with the same management interfaces commonly used to secure physical infrastructure. vShield Endpoint strengthens virtualization security with enhanced endpoint protection by offloading AV processing to a secure virtual appliance supplied by VMware partners. vShield Endpoint: - Improves consolidation ratios and performance by eliminating anti-virus "storms" - Automates anti-virus and anti-malware deployment and monitoring - Satisfies compliance and audit requirements with anti-virus and anti-malware activity logs In addition to the EPSEC APIs for antivirus/antimalware protection provided by vShield Endpoint, the VMware vCloud Ecosystem Framework provides service insertion at the vNIC and virtual edge level. This allows partner solutions to access both traffic flows and workload context without significant software development. Below is a list of partner-provided anti-malware and anti-virus solutions that are integrated with vCloud Networking and Security: - Juniper vGW Virtual Gateway - Kaspersky Anti-Virus - McAfee MOVE AV - Sophos Antivirus for vShield - Trend Micro Deep Security for vShield Endpoint
SoftLayer	SoftLayer's solution to protecting its customer from malware and viruses is by offering McAfee products: - McAfee LinuxShield Antivirus - McAfee Windows VirusScan Anti-Virus - McAfee AntiSpyware Customers may provision McAfee VirusScan Enterprise on any Windows server at no additional charge.

Requirement 8.16.3

- ✓ Please see Emergent's response to Requirement 8.6.4, specifically **Table 36** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.
- ✓ Please see Emergent's response to Requirement 8.7.1 with respect to managing the end of life activities of closing down a service.
- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider.

- ✓ Please see Emergent's response to Requirement 8.6.4, specifically **Table 36** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.
- ✓ Please see Emergent's response to Requirement 8.7.1 with respect to managing the end of life activities of closing down a service.
- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

Requirement 8.16.4

Ability to administer the solution in a distributed manner to different participating entities.

- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 6.5.3 with respect to **Table 8** identifying the service models, deployment models, and risk category for each of our proposed CSPs.
- ✓ Please see Emergent's response to Requirement 6.6 with respect to the scope and variety of the solutions we have proposed to offer under this solicitation.
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
- ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Requirement 8.16.5

Ability to apply a participating entity's defined administration policies in managing a solution.

- ✓ Please see Emergent's response to Requirement 8.6.4, specifically **Table 36** describing the policies and procedures each of our proposed CSPs has in place to ensure Purchasing Entities that access to user accounts or data is only to provide the service, including purposes compatible with providing the service and that it does not use customer data for advertising or similar commercial purposes.
- ✓ Please see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 6.5.3 with respect to **Table 8** identifying the service models, deployment models, and risk category for each of our proposed CSPs.
- ✓ Please see Emergent's response to Requirement 6.6 with respect to the scope and variety of the solutions we have proposed to offer under this solicitation.
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
- ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Requirement 8.17 (E) HOSTING AND PROVISIONING

Requirements 8.17.1 and 8.17.2

Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Provide tool sets at minimum for:

- 1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)*
 - 2. Creating and storing server images for future multiple deployments*
 - 3. Securing additional storage space*
 - 4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).*
-

Amazon Web Services

The AWS Management Console provides a web-based interface for accessing and managing AWS resources. Customers may also provision by means of the AWS SDKs and the AWS Mobile SDK, as well as through a wide range of 3rd party tools and gateways.

AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS resources and provision them in an orderly and predictable fashion. CloudFormation automates and simplifies the task of repeatedly and predictably creating groups of related resources to power applications.

Microsoft Azure

The Microsoft Azure portal is the unified hub that simplifies building, deploying, and managing cloud resources.

Resource Manager is a service that offers customers the ability to deploy, update or delete all of the resources for their solution in a single, coordinated operation using templates. Resource Manager provides security, auditing, and tagging features to help manage resources after deployment.

VMware vCloud Air vCloud Director orchestrates the provisioning of software-defined datacenter services to deliver complete virtual datacenters for easy consumption in minutes. Software-defined datacenter services and virtual datacenters fundamentally simplify infrastructure provisioning and enable IT to move at the speed of business.

- Deliver complete software-defined datacenter services as virtual datacenters
- Enable infrastructure to be ready for easy consumption in minutes
- Ensure workload security and automated resource control

SoftLayer The Customer Portal is an easy-to-use web interface for remotely managing SoftLayer services and accounts with access to more than 200 services, including the ability to:

- View performance details and control all functions of bare metal and virtual servers, easily turn a server off or on, view bandwidth graphs, ping servers to test network availability, reboot, etc.
- Manage account, set up billing information, change monthly billing methods, reset passwords, or add new users
- Deploy servers, firewalls, new backup solutions, and provision services to the environment

A lead-time of 2-4 hours is recommended when deploying bare metal servers.

- ✓ Please also see Emergent's response to Requirement 8.5.1 with respect to shared responsibilities.

Requirement 8.17.3

Ability to provide IaaS, PaaS, and SaaS solutions as defined service offerings with established rate structures

Emergent has submitted a copy of its authorization to resell services from each of our proposed CSPs as addenda to this proposal

- ✓ 10 Emergent LoA CH16012.pdf

Requirement 8.18 (E) TRIAL AND TESTING PERIODS (PRE- AND POST-PURCHASE)

Requirements 8.18.1, 8.18.2, 8.18.3

Describe your testing and training periods that your offer for your service offerings.

Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Offeror must describe what training and support it provides at no additional cost.

Amazon Web The AWS Free Tier is designed to enable potential customers to get hands-on experience with over 25 AWS Cloud Services. The AWS Free Tier includes

Services	services with a free tier available for 12 months following the AWS sign-up date, as well as additional service offers that do not automatically expire at the end of the 12 month AWS Free Tier term. AWS's free usage tier is not limited to specific use cases
Microsoft Azure	Microsoft offers a free one-month trial and a credit for up to \$200 to spend on all Azure services. During the trial, Microsoft will display the remaining trial credits at the top of the management portal.
VMware vCloud Air	VMware has various offers available listed on their "Special Offers" webpage.
SoftLayer	SoftLayer offers a 30-day trial period offered for SoftLayer services SoftLayer provides an environment for application testing that is needed to provide proof of concept. The environment will vary based on application requirements. SoftLayer will also provide infrastructure support services during the period of proof of concept testing at no additional cost.

Requirement 8.19 (E) INTEGRATION AND CUSTOMIZATION

Requirements 8.19.1 and 8.19.2

Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Each of our proposed CSPs can extend on-premises network configurations into virtual private networks. Resources will operate as if they are part of an existing corporate network. Customers can extend physical connectivity via dedicated, consistent, private networking between the data center and the CSPs regions they choose.

Table 44: Integration and Customization. Both open and proprietary solutions from our proposed CSPs can be customized and integrated to existing environments.

CSP	Integration and Customization of CSP Solutions
Amazon Web Services	Amazon Virtual Private Cloud (Amazon VPC). Within a logically isolated network, Amazon VPC provides complete control over the virtual networking environment, including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways. Amazon Direct Connect. AWS Direct Connect can establish a dedicated network connection between AWS and a customer's datacenter, office, or colocation environment. Data Integration and Lifecycle Management. Once the customer's architecture is connected to the cloud, AWS can ensure this data is reliably backed-up, help control where data is placed, replicate data across geographic regions, manage the lifecycle of data, or even have datacenter topology close enough to enable synchronous replication. AWS Storage Gateway. Available for download as a virtual machine (VM), customers install it on a host in the datacenter and use the AWS Management Console to create either Gateway-Cached or Gateway-Stored storage volumes that can be mounted as iSCSI devices by the on-premises applications.

	Amazon Simple Storage Service. A highly durable, scalable, and secure storage infrastructure that is well suited for backing up and archiving critical data. Amazon Glacier. Low-cost storage service providing secure and durable storage for data archiving and backup of data that is infrequently accessed and for which retrieval times of several hours are suitable. AWS Identity and Access Manager (AWS IAM). Supports identity federation for delegated access to the AWS Management Console or AWS APIs, such as an Amazon S3 bucket or an Amazon DynamoDB table. By integrating on-premises identity management and AWS, customers can quickly implement single sign-on (SSO), addition/deletion of users, and fine-grained AWS resource access using existing identity management solution. AWS Directory Service. A managed service that allows customers to connect AWS resources with an existing on-premises Microsoft Active Directory or to set up a new, stand-alone directory in the AWS Cloud. Integrated Resource and Deployment Management. AWS APIs allow for a wide variety of monitoring and management tools to integrate easily with AWS Cloud resources. Common tools from vendors such as Microsoft, VMware, BMC Software, Okta, RightScale, Eucalyptus, CA, Xceedium, Symantec, Racemi, and Dell already support AWS. AWS OpsWorks. An application management service to facilitate deploying and operating applications in the AWS Cloud or in the data center. Customers can define the application's architecture and the specification of each component, including package installation, software configuration, and resources. OpsWorks' integrates with Amazon CloudWatch as a single tool to create alarms or scale servers/instances based on CPU, memory, and load metrics in a hybrid environment. AWS CodeDeploy. A services to automate code deployments to instances, both in AWS and on-premises, to rapidly release new features, avoid downtime during deployment, and handle the complexity of updating applications. It eliminates the need for error-prone manual operations, and the service scales with infrastructure so customers can easily deploy to one instance or thousands.
Microsoft Azure	Microsoft provides a hybrid management solution for infrastructure and apps across private, partner, and public clouds. This means it's straightforward to move VMs to the Azure cloud and back again or to another cloud—including software licenses the customer already owns. • BizTalk Services. Provides out-of-the box, cloud to on-premises and line-of-business application integration for SAP, Oracle EBS, SQL Server, and PeopleSoft. Customer can connect with any HTTP, FTP, SFTP, or REST data source and route messages by using various Azure artifacts such as Service Bus queues, Topics, SQL Database, and Blob storage. • Hybrid Connections. A feature of BizTalk Services lets customers connect Azure Websites or Azure Mobile Services to any on-premises TCP or HTTP resource—such as Microsoft SQL Server, MySQL, or any web service—with just a few configuration changes and without using any custom code. Enterprise application integration with SaaS. Build applications on the cloud to integrate with SaaS applications as well as existing cloud-based applications. Model, build, and deploy cloud applications to quickly adapt to integration needs as they evolve. Use tools and portals for monitoring and managing integration flows. Build hybrid applications across cloud and on-premises. Couple the flexibility of cloud applications with on-premises data and services. Deploy hybrid applications with maximum agility – no need to configure a VPN, alter network perimeter or open up firewall.
VMware vCloud Air	VMware is virtualization software that runs on Microsoft Windows, Linux, and Mac OS X, while its enterprise software hypervisors for servers, VMware ESX and VMware ESXi, are bare-metal hypervisors that run directly on server hardware without requiring an additional underlying operating system. vCloud Air is a public/hybrid cloud platform built on the vSphere foundation, the proprietary technology behind VMware. Customers can leverage their existing VMware implementations to support their enterprise cloud computing objectives. vCloud Air supports more than 5,000 applications and 90+ operating systems certified to run on vSphere. The use of vCloud Air allows seamless workload portability and migration due to vSphere, which means no rewrites or recoding when moving workloads from an on-premise data center to the cloud and vice versa.
SoftLayer	SoftLayer's approach to integrating with other complimentary solutions was incorporated into the

	development of the service from Day 1. SoftLayer provides all services in a single, all API-driven management system. All SoftLayer data centers and network share a single, proprietary management system—every bare metal server, virtual server, storage device—in a single pane of glass and accessible by API, portal, and mobile applications. The SoftLayer API supports SOAP, XML-RPC, or REST protocols, C#, PERL, PHP, Python, Ruby, and VB.net API clients and provides granular control to manage integration and access with more than 3,000 documented methods across 180 discrete services. It's deployment tools provide seamless integration between virtual and bare metal servers, facilitate image imports and exports, dynamically adjust cloud footprint—even booting a failed server with an external kernel, to diagnose and resolve issues.

Requirement 8.20 (E) MARKETING PLAN

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

The Emergent marketing team creates and delivers nationwide campaigns to generate opportunities where our proposed CSPs solve the business challenges facing our state and local customers. Upon the award of a contract, Emergent will incorporate NASPO/ValuePoint into our marketing activities:

- **Nationwide Technology Events.** Emergent Technology Events are designed to share perspective on industry best practices and the proposed services provided by our CSPs helps public sector entities gain operational efficiencies, enforce regulatory compliance, reduce costs, and improve constituent services. In each Technology Event, attendees are presented information on one or more specific CSP.
- **Sponsorship and Access to High Profile Technologists.** Similar to our Nationwide Technology Events, we also provide access to some of the most well known technologists in the world. These events typically drive tremendous audiences, which affords us the opportunity to highlight the contract.
- **Trade Shows.** We invest in show room floors at trade shows throughout the country to showcase our full service capabilities—promoting new solutions and new contracts—to generate demand.
- **Virtual Technology Webinars.** Emergent hosts Virtual Technology Webinars as a service to our existing and prospective customers to learn more about the technology we represent. Each webinar is well attended and serves as a demand generation opportunity. We promote our contract vehicles as a part of our webinar series.
- **Dedicated Web and Social Media Support.** In support of a contract award, we will maintain a landing page featuring the NASPO/ValuePoint logos, links to the appropriate websites, a summary of contract and services offered, as well as any due diligence documents including, but not limited to a copy of solicitation, a copy of contract and any amendments, and marketing materials. In addition, Emergent will provide a soft-copy Contract Guide explaining the contact's quote and ordering procedures. Other web and social media promotions will include Twitter, Facebook, and LinkedIn.
- **Formal Press Releases and Promotions via Emergent News.** Emergent support of the NASPO/ValuePoint program will be released as a formal press release—subject to approval approval—to the US News one newswire via PR Newswire. These announcements generate

visibility and are archived on our own news site to help promote the contract. Further press release will be generated to support marketing initiatives.

- **Collateral and Campaigns.** Working in conjunction with our marketing team, we will develop collateral to enable us to effectively communicate the benefits of the contract to our current customers including the pricing and additional value offered through the contract. Campaigns, including direct mail, advertisements in regional or national publications, and participation in trade shows, will feature prominent NASPO/ValuePoint placements.

Commitment to NASPO/ValuePoint

- **Corporate.** Emergent will direct traditional “open market” sales to the contract, and, where beneficial to an eligible participant, present the contract as our preferred acquisition vehicle.
- **Pricing.** When leading with the NASPO/ValuePoint contract, Emergent will seek approvals from our CSPs to extend potential deeper discounts to eligible participants.
- **Economic.** Emergent will demonstrate the benefits, including the incorporated terms, contract scope and pricing advantage, of the contract over alternative options, including competitive solicitations, as a more effective alternative to the cost and time associated with such alternate bids and solicitations.
- **Sales.** Emergent sales force will be properly trained and incentivized to lead with the NASPO/ValuePoint contract.

Marketing the NASPO/ValuePoint Master Agreement

Emergent sales and marketing teams will take a proactive, multifaceted approach to marketing the contract into the primary offering to eligible participants. To initially understand the messaging that Emergent will convey to eligible participants, Emergent will first complete an analysis of our current customer base against eligible participants. After our analysis, we will have three customer groups that we will be able to create a tailored and direct marketing outreach program for:

- **Group 1.** Eligible participants: CSP and Emergent Customers
- **Group 2.** Eligible participants: non-CSP and non-Emergent Customers
- **Group 3.** Eligible participants: Emergent Customers

With this information, Emergent has the ability to create various marketing campaigns aimed at informing eligible participants of Emergent’s recent award for providing cloud services. For eligible participants that are current CSP and Emergent customers, we can reach out them directly to discuss the recent award to Emergent and how we can begin transitioning them to the contract for their cloud computing needs. For eligible participants that are not current CSP or Emergent customers, we will target each to inform them about the contract as well as provide an overview of each of our proposed CSP offerings to identify any current needs or requirements.

Emergent will accomplish our targeted out-reach to the various customers groups with outbound call campaigns, direct marketing initiatives utilizing Emergent/CSP/NASPO/ValuePoint branded

collateral and with our general marketing approach of utilizing social media and live in-person national technology days.

Sales Enablement

Emergent has an effective and streamlined process to educate our national sales force on new contracts and solutions being launched to better serve Emergent customers and partners. Internal “Sales Enablement” trainings are co-developed between the Emergent Sales organization and Marketing department to communicate the value of new contracts. Each training session details the value of the new contract to a customer, to Emergent, to our partner CSPs, and to the sponsoring agency, as well as how and where to best position the it for maximum use. Specific tools used to educate the national sales force include:

- **Sales Enablement Contract Review.** Emergent produces and hosts a mandatory contract training webinar to cover best practices that drive more product sales.
- **Sales Enablement Contract Summary Collateral.** Emergent creates summary contract collateral and reference materials for our internal sales teams as well as our exiting and potential customers. Each contract collateral piece includes:
 - ✓ Contract Title
 - ✓ Contract Number and Formal Description
 - ✓ Summary Overview of the Contract
 - ✓ Contract Offering (Products)
 - ✓ Contract Offering (Services)
 - ✓ Detailed Contact Information
 - ✓ Emergent Contract Program Manager
 - ✓ Emergent Contract Executive Sponsor
 - ✓ Specialized Contract Contact Information per contract that may include (Consulting and or Training Contacts where appropriate).

Emergent sales teams utilize collateral to highlight and briefly describe our organization, featured CSP products, service offerings and contracts. These marketing aids well help assist in our outreach to customers but also serve as a constant reminder of the NASPO/ValuePoint contract.

Requirement 8.21 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

Supporting our Cloud and Security Sales team are technical architects, deployment engineers and PMP project managers. Our architects, engineers, and project managers are taken from the pool of over 100 W-2 employees that make up our parent company’s consulting organization, Mythics Consulting.

We haven’t come across another *reseller* that dedicates 40% of its organization to perform services for the public sector—but when you add up the number of employees between Mythics and Emergent, that’s what you get. Nor have we found one that embraces an industry standard delivery methodology and a globally recognized quality management system to deploy technical resources with so many applicable certifications.

- **Certifications.** Because our parent company, Mythics is 100% dedicated to selling Oracle products and product enhancing services, our customers expect our resources to have Oracle certifications. We give them more. Almost all of our consultants hold additional certifications relevant to their roles—PMI, PMI, CSM, ITIL, Six Sigma, among others. Many of them have received certifications in other technologies relevant to NASPO's contemplated contract.
- **Delivery Methodology.** We assign a PMP-certified project manager to every consulting engagement so that we deliver projects in accordance with the best practices as codified by the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK)
- **Quality Management System.** We don't deliver projects any other way, because our entire delivery methodology—from initial opportunity identification to project close adheres to our independently audited Quality Management System—which is registered to the ISO 9001:2008 standard.

Requirement 8.22 (E) SUPPORTING INFRASTRUCTURE

Requirement 8.22.1 and 8.22.2

Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

If required, who will be responsible for installation of new infrastructure and who will incur those costs?

- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 6.5.3 with respect to **Table 8** identifying the service models, deployment models, and risk category for each of our proposed CSPs.
- ✓ Please see Emergent's response to Requirement 6.6 with respect to the scope and variety of the solutions we have proposed to offer under this solicitation.
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
- ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.

Requirement 8.23 (E) ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

- ✓ Please see Emergent's response to Requirement 6.4.1 where Emergent has mapped the applicable service models to the great depth and breadth our proposed offerings in **Table 4**.
- ✓ Please see Emergent's response to Requirement 6.5.3 with respect to **Table 8** identifying the service models, deployment models, and risk category for each of our proposed CSPs.
- ✓ Please see Emergent's response to Requirement 6.6 with respect to the scope and variety of the solutions we have proposed to offer under this solicitation.

-
- ✓ Please see Emergent's response to Requirement 8.1.2 with respect to meeting NIST SP 800-145 essential characteristics.
 - ✓ Please see Emergent's response to Requirement 8.1.3 with respect to mapping the Service Model subcategories to each of our proposed CSPs' SaaS, PaaS, and IaaS offerings.



Section Title: Confidential, Protected or Proprietary Information

All confidential, protected or proprietary Information must be included in this section of proposal response.

Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write "None" in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

None

Section Title: Exceptions and/or Additions to the Standard Terms and Conditions

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations.

If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

EMERGENT, LLC LIST OF EXCEPTIONS TO NASPO VALUEPOINT TERMS AND CONDITIONS

For Utah Solicitation Number CH16012

March 10, 2016

Emergent, LLC ("Emergent") wishes to take exception to several provisions in the NASPO VALUEPOINT Terms and Conditions for Utah Solicitation Number CH16012 (the "Solicitation"). In the subsequent paragraphs Emergent has delineated the specific clauses in the solicitation's terms and conditions to which it wishes to take exception.

1. Under Section 1 of the Solicitation, Emergent takes exception to the following statement: "If any provision of this RFP conflicts with the UCA or UAC, the UCA or UAC will take precedence." Such codes shall only take precedence with respect to procurement laws and shall not apply to Emergent if they solely apply to Purchasing Entities and/or government functions.

2. Under Section 3.4 of the Solicitation, Emergent takes exception to the following statement: "Offerors may not submit requests for exceptions and/or additions by reference to an Offeror's website or URL. URLs provided with a proposal may result in that proposal being rejected as non-responsive." Emergent is providing website links and/or URLs in its response due to the overwhelming volume of documents we are providing, since we are a reseller and our offering is comprised of services supplied by several different manufacturers. As a result, such website links and/or URLs may be necessary and reasonable to clarify certain, applicable manufacturer terms and conditions. In addition, such links and/or URLs are being provided for current informational purposes only and Emergent bears no responsibility for the accuracy, legality or content of the information, which is in the control of and subject to change by the applicable manufacturers as terms and conditions will evolve over time in accordance with updates to the manufacturer offerings. Furthermore, certain manufacturers may be submitting their own responses to the Solicitation and in that event there may be a requirement by a manufacturer to have the terms and conditions that it directly negotiated apply to resellers too with respect to any awards resulting from this Solicitation.

3. Under Section 5.7 of the Solicitation, Emergent takes exception to the following statement: "Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its

proposal.” Emergent is willing to annually meet with the Lead State to determine whether or not the services offered meet or exceed the technical capabilities stated in Emergent’s response to the Solicitation, since the manufacturers’ services will evolve over time and Emergent cannot control the manner in which they will evolve.

4. Under Section 8.13, Emergent takes exception to the requirement to provide a certification, since we are a reseller and some of the manufacturers of the services we are offering may not represent and warrant the accuracy of the applicable documents. Emergent will only be able to provide what the manufacturers provide.

5. Under Section 1 of Attachment A to the Solicitation, Emergent takes exception to the order of precedence. The Emergent response should be number two in the order of precedence, since the Emergent response will contain exceptions to the Solicitation, which if negotiated and mutually agreed upon by the parties would control over Attachment A and the other Solicitation terms and conditions that were modified by such agreement. Such negotiated and mutually agreed upon terms and conditions will include the applicable manufacturer terms and conditions referenced in Emergent’s response. In addition, Emergent reserves the right to review the terms and conditions in each Participating Addendum and any individual purchase orders and to negotiate additional and/or other terms and conditions, which shall be mutually agreed upon by the parties and shall supersede Attachment A and the other Solicitation terms and conditions.

6. Under Section 2 of Attachment A to the Solicitation, Emergent takes exception to the definition of “Confidential Information”. The definition should apply to information of both the Purchasing Entity and the Contractor. In addition, the definition is subject to how it is defined in the applicable manufacturer’s terms and conditions. However, at a minimum, Emergent requests the following definition instead: “Confidential Information” is non-public information that is marked or identified at the time of disclosure as “confidential” or that a reasonable person should understand to be confidential, including, but not limited to: (1) Customer Data; (2) any Purchasing Entity’s records, (3) personnel records, and (4) information concerning individuals.”

7. Under Section 2 of Attachment A to the Solicitation, Emergent takes exception to the definition of “Data”. The current definition is broad and includes metadata, which is different than the data placed into a product by a Purchasing Entity. As a result, the definition needs to be subject to how it is defined in the applicable manufacturer’s terms and conditions.

8. Under Section 2 of Attachment A to the Solicitation, Emergent takes exception to the definitions of “Data Breach” and “Security Incident”, since some manufacturers may not have separate definitions and/or processes for notification and mitigation for such terms. As a result, the definitions need to be subject to how it is defined in the applicable manufacturer’s terms and conditions.

9. Under Section 2 of Attachment A to the Solicitation, Emergent takes exception to the definition of “Protected Health Information”, since it is subject to change by updates to applicable statute and should only apply to information stored and processed by the services. However, storage and processing may differ by manufacturer and since Emergent is offering several services by different manufacturers the definition needs to be subject to how it is handled by the applicable manufacturer’s terms and conditions.

10. Under Section 2 of Attachment A to the Solicitation, Emergent takes exception to the definition of “Service Level Agreement”, since each manufacturer will have its own Service Level Agreement that is not typically negotiable due to the fact that manufacturers have to have a consistent means to administer its Service Level Agreement across all of its customers. As a result, Emergent requests the following definition instead: “Service Level Agreement” (SLA) means the applicable manufacturer document which specifies the standards to which the manufacturer agrees to adhere and by which it measures the level of service for its services. The then current version of the manufacturer’s SLA shall apply at the time of purchase and will be provided to the Purchasing Entity at such time.”

11. Under Section 7 of Attachment A to the Solicitation, Emergent takes exception to the fact that no cure period is provided for breach and that the provision does not capture the fact that the Purchasing Entity may have obligations with respect to Termination and Suspension of Service in accordance with the applicable manufacturer's terms and conditions. As a result, Emergent requests the following revised provision: “Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance of an applicable Service Level Agreement in association with any Order, obligations under Termination and Suspension of Service in accordance with the applicable manufacturer’s terms and conditions, and any responsibilities arising out of a Security Incident or Data Breach in accordance with the applicable manufacturer’s terms and conditions. Termination of the Master Agreement due to Contractor default may be immediate if defaults cannot be reasonably cured as allowed per Default and Remedies terms.”

12. Under Section 8 of Attachment A to the Solicitation, Emergent takes exception to the fact that the provision is not mutual. The Confidential Information of both parties should be covered. Also, this provision will need to be subject to the applicable manufacturer's procedures for protection and return of information. Furthermore, manufacturers will limit their liability with respect to Security Incidents and/or Data Breaches, so Emergent requests that the following subsection be added to the end of this provision: “e. Notwithstanding the foregoing, damages attributable to a Data Breach and/or Security Incident, which definitions are subject to the

applicable manufacturer terms and conditions, shall be subject to the Section of the Master Agreement titled "Limitation of Liability."

13. Under Section 10 of Attachment A to the Solicitation, Emergent takes exception to the fact that the provision is not mutual. As a result, at a minimum subsections (b) and (c) need to be revised to apply to both parties, so that each party has a right to claim a default and issue written notice of default to the other party. Also, the provision needs to be subject to the applicable manufacturer's terms and conditions regarding termination of services. Furthermore, with respect to subsection (a)(3), Emergent disclaims information found at any manufacturer links, because Emergent does not control such information and as a result can bear no responsibility with respect to such information.

14. Under Section 13 of Attachment A to the Solicitation, Emergent takes exception to the overly broad indemnification provision. Emergent only provides the indemnification furnished by the applicable manufacturer of the offered services for the offered services, which is set forth in the manufacturer's terms and conditions. Also, the manufacturer's indemnification provision may be subject to a limitation of liability in accordance with the applicable manufacturer's terms and conditions.

15. Under Section 17 of Attachment A to the Solicitation, Emergent takes exception to the broad compliance with laws statement, since the applicable manufacturers may have specific statements regarding their compliance with applicable laws. As a result, this provision shall be subject to the applicable manufacturer's terms and conditions.

16. Under Section 19 of Attachment A to the Solicitation, the term "Service Level Agreement" is subject to the exception stated above in number ten. The reference to "Service Level Agreement" shall mean the applicable manufacturer's Service Level Agreement.

17. Under Section 22 of Attachment A to the Solicitation, Emergent takes exception to the statement that information cannot be shared with third parties. Since Emergent is responding to this Solicitation as a reseller, Emergent will need to share data with the applicable manufacturer in accordance with the manufacturer's terms, which may not have an annual instruction requirement.

18. Under Section 23 of Attachment A to the Solicitation, Emergent takes exception to the required maintenance, since it will be subject to the applicable manufacturer's terms and conditions for maintenance of such items.

19. Under Section 25 of Attachment A to the Solicitation, Emergent takes exception to the restrictions on use, since metadata may be used by the applicable manufacturer in accordance with the applicable manufacturer's terms and conditions.

20. Under Section 28 of Attachment A to the Solicitation, Emergent takes exception to the “best efforts” requirement, since Emergent will only be able to provide restoration in accordance with the applicable manufacturer's terms and conditions.

21. Under Section 29 of Attachment A to the Solicitation, Emergent takes exception to the required license. Any license grant will be subject to the applicable manufacturer's terms and conditions.

22. Under Section 30 of Attachment A to the Solicitation, Emergent takes exception to the data privacy requirements, since Emergent will only be able to comply in accordance with the extent that the applicable manufacturer can comply as set forth in the applicable manufacturer's terms and conditions.

23. Under Section 31 of Attachment A to the Solicitation, Emergent takes exception to the warranty requested. Emergent will only provide the warranty furnished by the applicable manufacturer of the offered services, which is set forth in the manufacturer’s terms and conditions. Furthermore, there is no disclaimer in this section. As a result, Emergent requests that the following be included at a minimum as the warranty disclaimer: “THE MANUFACTURER WARRANTIES ARE THE ONLY EXPRESS WARRANTIES PROVIDED BY EMERGENT. EMERGENT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESSED, STATUTORY OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY AND ALL WARRANTIES IMPLIED FROM CUSTOM, USAGE IN TRADE OR COURSE OF DEALING.” Also, Emergent disclaims information found at manufacturer links, because Emergent does not control such information and can bear no responsibility with respect to such information. Furthermore, access and use to the services are subject to the applicable manufacturer's terms and conditions, including, but not limited to non-payment issues (e.g., possible right to suspend services).

24. Under Section 32 of Attachment A to the Solicitation, Emergent takes exception to the requirement to provide transition assistance at no additional cost. This provision will need to be subject to the applicable manufacturer's terms and conditions, because additional costs may apply for such assistance.

25. Under Section 33 of Attachment A to the Solicitation, Emergent takes exception to the fact that the provision is not mutual. The requirements regarding waivers should apply to both parties.

26. Under Section 41 of Attachment A to the Solicitation, Emergent takes exception to the fact that no government support should be expected. Individual orders could require that the Purchasing Entity have certain equipment, etc., so this provision needs to be subject to the applicable manufacturer's terms and conditions regarding items required to be furnished by the Purchasing Entity.

27. Emergent takes exception to the fact that there is no limitation of liability provision in the Master Agreement. As a result, Emergent requests that the following be added as a new Section 42 to Attachment A: "Emergent's limitation of liability shall be as set forth in the applicable manufacturer's terms and conditions. If no such limitation is set forth in the applicable manufacturer's terms and conditions, then the following language shall apply: "IN NO EVENT SHALL EMERGENT BE LIABLE FOR LOSS OF USE, LOSS OF DATA, LOSS OF REVENUE, INTERRUPTION OF BUSINESS, LOST PROFITS, ANY COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES OF ANY KIND UNDER ANY CAUSE OR ACTION (INCLUDING CONTRACT, TORT or STRICT LIABILITY) arising from or out of the CONTRACT. IN ADDITION, EMERGENT'S total liability HEREUNDER, REGARDLESS OF THE form of action (INCLUDING CONTRACT, TORT OR STRICT LIABILITY), will in no event exceed ANY LOSS, DAMAGE, COST, EXPENSE OR LIABILITY ARISING IN RESPECT TO THE FEES PAID by A PURCHASING ENTITY TO EMERGENT FOR THE SERVICES during the twelve (12) month period immediately preceding the event giving rise to the liability. FURTHERMORE, THE LIMITATIONS SET FORTH IN THIS SECTION ARE INDEPENDENT OF ANY LIMITED REMEDY SET FORTH HEREIN, SHALL APPLY WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY."

28. With respect to the Exhibits to the Solicitation, Emergent takes exception to the terms and conditions that are in conflict with the applicable manufacturer terms and conditions, since many items covered in the Exhibits pertain to specific service functionality.

Section Title: Cost Proposal

Cost Proposals will be evaluated independently from the technical proposal. Offeror's cost proposal must include the items discussed in Section 9 of the RFP.

Cost will be evaluated independently from the Mandatory Minimum Requirements, and the Technical responses. Inclusion of any cost or pricing data within the Detailed Technical Proposal will result in the proposal being judged as non-responsive for violation of UCA § 63G-6a-707(5).

All costs incurred by an Offeror in the preparation and submission of a proposal, including any costs incurred during interviews, oral presentations, and/or product demonstrations are the responsibility of the Offeror and will not be reimbursed by the Lead State or NASPO ValuePoint.

9.1 (M) COST PROPOSAL

Given that technology products generally depreciate over time and go through typical product lifecycles, it is more favorable for Purchasing Entities to have the Master Agreement be based on minimum discounts off the Offeror's commercially published pricelists versus fixed pricing. In addition, Offerors will have the ability to update and refresh their respective price books, as long as the agreed-upon discounts are fixed. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

Offeror must identify its cost proposal, Attachment G, as "Cost Proposal – CH16012 Cloud solutions". No specific format is required for an Offeror's price schedule; however the Offeror must provide and list a discount from its pricing catalog. New discount levels may be offered for new services that become available during the term of the Master Agreement, as allowed by the Lead State.

Pricing catalogs should include the price structures of the cloud solutions models and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing must be all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

The Lead State understands that each Offeror may have its own pricing models and schedules for the Services described in the RFP. It is the intent to of the RFP to allow price schedules that are viewed in the traditional line item structure or price schedule that have pay-as-you-go characteristics.

An Offeror's price catalog should be clear and readable. Participating Entities, in reviewing an Offeror's Master Agreement, will take into account the discount offered by the Offeror along with the transparent, publicly available, up-to-date pricing and tools that will allow customers to evaluate their pricing.

Individual Participating Addendums will use the cost proposals pricing as a base and may negotiate an adjusted rate.

Offeror's price catalog should be broken into category for each service category. For example if an Offeror provides a SaaS offering then its price catalog should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Some Participating Entities may desire to use an Offeror for other related application modifications to optimize or deploy cloud solutions applications. Responses to the RFP must include hourly rates by job specialty for use by Participating Entities for these types of database/application administration, systems engineering & configuration services and consulting throughout the contract period. The hourly rates should be a fully burdened rate that includes labor, overhead, and any other costs related to the service. The specific rate (within a range) charged for each proposed contracted service would be the lowest rate shown unless justified in writing and approved by the Lead State. Any of these valued-added services must be included in your cost proposal, e.g., by an hourly rate.

Emergent has submitted Cost Proposal form as addenda to this proposal:

✓ 11 Emergent Cost Proposal CH16012.pdf

ⁱ [Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, 18 May 2015](#)

ⁱⁱ [Gartner Magic Quadrant for Enterprise Application Platform as a Service, Worldwide, 24 March 2015](#)

ⁱⁱⁱ [The Forrester Wave™: Enterprise Public Cloud Platforms, Q4 2014](#)

10 March 2016

Christopher Hughes, Assistant Director
State of Utah, Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Subject: NASPO ValuePoint and the State of Utah Request for Proposal CH16012 Cloud Solutions

Mr. Hughes,

Emergent is pleased to present to you a proposal that will demonstrate that Emergent is fully qualified and available to provide the cloud solutions required for this contract to be successful and the best value for NASPO/ValuePoint.

As requested in the RFP document, Mythics attests to the following:

Requirement 5.2.1

A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

Emergent understands that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

Requirement 5.2.2

A statement naming the firms and/or staff responsible for writing the proposal.

The following Emergent staff was responsible for writing this proposal:

- James Flint
- Lynn Brogis
- Venkat Sundaram

Emergent also received content from Amazon Web Services and SoftLayer.

Requirement 5.2.3

A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

Emergent is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

Requirement 5.2.4

A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

Emergent acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

Requirement 5.2.5

A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.

Emergent is capable of providing the following cloud offerings under the terms of the RFP.

Table 1: NIST Cloud Computing Service and Deployment Models. *Emergent's proposed cloud solutions meet the requirements of NIST SP 800-145.*

Cloud Service Provider	Service Model(s)	Deployment Model(s)	Risk Category
Amazon Web Services	IaaS, PaaS, SaaS	Public	Moderate
Microsoft Azure	IaaS, PaaS, SaaS	Public	Moderate
VMware vCloud Air	IaaS, PaaS, SaaS	Public, Hybrid	Moderate
SoftLayer	IaaS	Private, Public, Hybrid	Moderate

All of our proposed CSPs offer SaaS, PaaS, and IaaS having received either Joint Authorization Board (JAB) Provisional Authorization or an Agency FedRAMP Authorization. In the spirit of the “do once, use many times”, for each proposed offering, Emergent has identified the applicable NIST Cloud Computing Service and Deployment Models as approved by FedRAMP.

NOTE: FedRAMP Authorization is not necessarily applicable to other solutions found in each CSP’s respective Marketplace.

Table 2: Service Model Subcategories. *Our proposed CSPs provide a wide range of SaaS, PaaS, and IaaS offerings.*

Service Model/Subcategory	Amazon Web Services	Microsoft Azure	VMware vCloud Air	SoftLayer
IaaS: Computer/Infrastructure Services/Operating systems	Yes	Yes	Yes	Yes
IaaS: Computer/Infrastructure Services/Hypervisors	Yes	Yes	Yes	Yes
IaaS: Disaster Recovery/Business Continuity	Yes	Yes	Yes	Yes

IaaS: Disaster Recovery/High Availability / Failover	Yes	Yes	Yes	Yes
IaaS: GIS	Yes	Yes	Marketplace	Marketplace
IaaS: Storage/File	Yes	Yes	Yes	Yes
IaaS: Storage/Block	Yes	Yes	Yes	Yes
IaaS: Storage/Object	Yes	Yes	Yes	Yes
IaaS: Storage/Archive	Yes	Yes	Yes	Yes
IaaS: Storage/Cache	Yes	Yes	Yes	Yes
IaaS: Storage/Content Delivery Networks (CDN)	Yes	Yes	Yes	Yes
IaaS: Storage/Litigation Hold	Yes	Yes	Yes	Marketplace
IaaS: Network/Virtual network	Yes	Yes	Yes	Yes
IaaS: Network/Load balancer	Yes	Yes	Yes	Yes
IaaS: Network/DNS	Yes	Yes	Yes	Yes
IaaS: Network/Gateway (e.g. VPN or Application)	Yes	Yes	Yes	Yes
IaaS: Network/Firewall	Yes	Yes	Yes	Yes
IaaS: Network/Traffic manager	Yes	Yes	Yes	Yes
IaaS: Network/Direct link	Yes	Yes	Yes	Yes
IaaS: PC/Desktop "aaS"	Yes	Yes	Yes	Marketplace
IaaS: Security/Identity & Access Management	Yes	Yes	Yes	Yes
IaaS: Security/Encryption	Yes	Yes	Yes	Yes
IaaS: Security/Data Loss Prevention (DLP)	Yes	Yes	Yes	Yes
IaaS: Security/Web Security	Yes	Yes	Yes	Yes
IaaS: Security/Email Security	Yes	Yes	Yes	Yes
IaaS: Security/Network Security	Yes	Yes	Yes	Yes
IaaS: Security/Security Information and Event Management (SIEM)	Yes	Yes	Yes	Yes
IaaS: Security/Intrusion Management	Yes	Yes	Yes	Yes
IaaS: Security/DDOS Monitoring / Management	Yes	Yes	Yes	Yes
IaaS: Other (identify additional sub-categories and/or descriptors)	Yes	Yes	Yes	Yes
PaaS: Analytics/Hadoop	Yes	Yes	Yes	Yes
PaaS: Analytics/Business Intelligence	Yes	Yes	Marketplace	Marketplace
PaaS: Analytics/Data Warehouse	Yes	Yes	Yes	Yes
PaaS: Database/Relational	Yes	Yes	Yes	Yes
PaaS: Database/NoSQL	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Containers	Yes	Marketplace	Yes	Yes
PaaS: Development, Testing and Deployment/Services and APIs	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Mobile	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Internet of Things	Yes	Yes	Yes	Yes
PaaS: Development, Testing and Deployment/Tools	Yes	Yes	Yes	Yes

PaaS: Development, Testing and Deployment/Runtime environments	Yes	Yes	Yes	Yes
PaaS: Electronic Records Management	Marketplace	Marketplace	Marketplace	Yes
PaaS: E-Discovery	Marketplace	Marketplace	Marketplace	Yes
PaaS: GIS	Marketplace	Marketplace	Marketplace	Yes
PaaS: Integration (iPaaS)	Yes	Yes	Yes	Yes
PaaS: Open Source	Yes	Yes	Yes	Yes
PaaS: Other (identify additional sub-categories and/or descriptors)	Gaming, Mobile, Desktop	Marketplace	Marketplace	Yes
SaaS: Data Analytics	Yes	Yes	Marketplace	Yes
SaaS: Business Intelligence	Yes	Yes	Marketplace	Yes
SaaS: Business Continuity/Disaster Recovery	Yes	Yes	Marketplace	Yes
SaaS: Cloud and Infrastructure Management Tools	Yes	Yes	Marketplace	Yes
SaaS: Collaboration	Marketplace	Yes	Marketplace	Yes
SaaS: Customer Relationship Management	Marketplace	Yes	Marketplace	Yes
SaaS: Citizen Relationship Management	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Data Management	Yes	Yes	Marketplace	Yes
SaaS: E-Discovery	Marketplace	Marketplace	Marketplace	Yes
SaaS: Electronic Records Management	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace
SaaS: ERP/HR	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Finance	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Budget	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: ERP/Procurement	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace
SaaS: GIS	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Human Resource/Payroll	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Human Resource/Time, Attendance and Scheduling	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Human Resource/Recruitment and Hiring	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Internet Filtering	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Licensing and Registration Systems	Marketplace	Yes	Marketplace	Yes; also in Marketplace
SaaS: Office Productivity/Word Processing	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Document Tracking	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/E-mail	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Spread sheets	Yes	Yes	Marketplace	Yes
SaaS: Office Productivity/Presentation	Yes	Yes	Marketplace	Yes
SaaS: Message Filtering	Yes	Yes	Marketplace	Yes
SaaS: Meeting Planning, hosting, conferencing	Marketplace	Yes	Marketplace	Yes

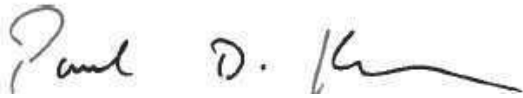
SaaS: Mobile Data Management	Marketplace	Yes	Marketplace	Yes
SaaS: Point of Sale (POS)	Yes	Yes	Marketplace	No
SaaS: Procurement Systems	Marketplace	Marketplace	Marketplace	Marketplace
SaaS: Project and Portfolio Management (PPM) Tools.	Marketplace	Yes	Marketplace	Yes
SaaS: Security	Yes	Yes	Yes	Yes
SaaS: Travel Management	Marketplace	Yes	Marketplace	Marketplace
SaaS: Workflow and Electronic Signature	Marketplace	Yes	Marketplace	Marketplace
SaaS: Other (identify additional sub-categories and/or descriptors)	Marketplace	Marketplace	Marketplace	Yes; also in Marketplace

Requirement 5.2.6

A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.

- ✓ Please see Emergent's response to Requirement 5.2.5, specifically **Table 1** identifying the data risk categories that our proposed CSPs are capable of storing.

Respectfully,



Paul Kohler

Executive Vice President

Emergent, LLC

Attachment E – Applicable Manufacturer Terms and Conditions

Exhibit 1. Applicable Manufacturers. Providers of commercially-available cloud solutions available for purchase under this Master Agreement (Applicable Manufacturers) —as well as Applicable Manufacturer Terms and Conditions are set forth in the table below:

Applicable Manufacturer	Applicable Manufacturer Terms and Conditions
Amazon Web Services	Exhibit 2, inclusive of: “AWS Public Sector Access Policy (State)”
Microsoft Azure	Exhibit 3, inclusive of: “Microsoft Cloud Agreement” “Microsoft Online Services Terms – January 2017” “Microsoft Product Terms – January 2017” “Microsoft SLA – January 2017”
IBM/SoftLayer	Exhibit 4, inclusive of: “Service Description: IBM Bluemix” “SoftLayer: Cloud Service Agreement” “Service Description: IBM Bluemix Managed Hosting” “IBM Data Processing Addendum (with EU Standard Contractual Clauses) (<i>Final Version November 2016</i>)”



Exhibit 2. Applicable Terms and Conditions for Amazon Web Services.

AWS PUBLIC SECTOR ACCESS POLICY (STATE)

(Last Updated March 17, 2016)

This AWS Access Policy ("**Access Policy**") governs your access to and use of the Services (as defined below) of Amazon Web Services, Inc. ("**AWS**") provided to you by your systems integrator, reseller, or services provider ("**Provider**"). It sets out the additional rules, conditions and restrictions that apply to you or the entity you represent ("**you**") for use of the Services. In this Access Policy, "**we**", "**us**", or "**our**" means AWS and any of its affiliates. Please see Section 10 for definitions of capitalized terms.

1. Use of the Services.

1.1 Generally. You are provided access to the Services by your Provider. Your use of and access to the Services are governed by the agreement between you and Provider. This Access Policy supplements the terms of such agreement and may be updated by us from time to time. AWS Service Level Agreements do not apply to your use of the Services. Your continued access to and use of the Services is conditioned on your compliance with all laws, rules, regulations, policies and instructions applicable to your use of the Services, including the Policies.

1.2 Account Keys. Provider may provide you with AWS account keys which will allow you to directly access the Services via Provider's account(s). We are not responsible for any activities that occur under these account keys, regardless of whether the activities are undertaken by you, Provider or a third party (including your employees, contractors or agents) and we are also not responsible for unauthorized access to the account.

1.3 Third Party Materials. Through the use of Provider's AWS account(s), you may have access to Third Party Materials, such as software applications provided by third parties, which are made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Your use of any Third Party Materials is at your sole risk.

2. Your Responsibilities.

2.1 Your Materials. You are solely responsible for the development, content, operation, maintenance, and use of Your Materials with the Services. For example, you are solely responsible for:

(a) the technical operation of Your Materials, including ensuring that calls you make to any Service are compatible with then-current application program interfaces for that Service;

(b) compliance of Your Materials with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Materials;

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Materials violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act;

(e) any action that you permit, assist or facilitate any person or entity to take related to this Access Policy, Your Materials or use of the Services; and

(f) End Users' use of Your Materials and the Services and ensuring that End Users comply with your obligations under this Access Policy and that the terms of your agreement with each End User are consistent with this Access Policy.

2.2 Other Security and Backup. You or Provider are solely responsible for properly configuring and using the Services and taking steps to maintain appropriate security, protection and backup of Your Materials, including using encryption technology to protect Your Materials from unauthorized access and routinely archiving Your Materials.

2.3 End User Violations. If you become aware of any violation of your obligations under this Access Policy by an End User, you will immediately terminate such End User's access to Your Materials and the Services.

3. Service Interruption.

3.1 General. We may suspend the AWS account(s) through which you access the Services immediately if we determine your or an End User's use of the Services (i) violates the terms of this Access Policy (including the Acceptable Use Policy or Service Terms); (ii) poses a security risk to the Services or any other AWS customer, (iii) may harm our systems or the systems or Materials of any other AWS customer; or (iv) may subject us to liability as a result of any of the foregoing. We will provide notice of any suspension as soon as practicable to Provider, who is solely responsible for providing any notices to you under your agreement with them.

3.2 Scope of Interruption. To the extent practicable, we will (i) suspend your right to access or use only those instances, data, or portions of the Services that caused the suspension, and (ii) limit the suspension to those accounts that caused the suspension. If commercially feasible, access to the Services will be restored once the conditions or circumstances giving rise to the suspension have been removed or corrected. Nothing in this Section 3 will operate to limit your rights or remedies otherwise available to you against Provider under your agreement with them or applicable law.

4. Proprietary Rights.

4.1 Services. As between you and us, we or our licensors own and reserve all right, title, and interest in and to the Services. You have the right to use the Services solely as a licensee of Provider in accordance with this Access Policy and the agreement between you and Provider. We have no obligation to provide the Service to you under this Access Policy, so you must look exclusively to Provider and your agreement with Provider regarding such obligation. Except as expressly provided in this Section 4, you obtain no rights to the Services, the AWS Materials or any Third Party Materials.

4.2 Materials. As a part of the Services, you may have access to AWS Materials and Third Party Materials, which may be subject to additional terms and conditions (including the Terms of Use and Apache Software License). By using those materials, you are subject to such additional terms. You are solely responsible for securing any necessary approvals for the download and use of such materials.

4.3 Restrictions. Neither you nor any End User may use the Services in any manner or for any purpose other than as expressly permitted by this Access Policy and the agreement between you and Provider. Neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the Services (except to the extent software included in the Services are provided to you under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the software included in the Services or apply any other process or procedure to derive the source code of any software included in the Services, or (c) access or use the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas. All rights and access granted to you with respect to the Services are conditioned on your continued compliance with this Access Policy, and you will immediately discontinue your use of the Services if you cannot comply with this Access Policy. You will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our customers, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding any Services or AWS Materials that you have used.

4.4 Suggestions. If you provide any Suggestions to us when using the Services, you hereby grant to AWS and its affiliates a perpetual, irrevocable, non-exclusive, worldwide, royalty-free right and license to reproduce, distribute, make derivative works based upon, publicly display, publicly perform, make, have made, use, sell, offer for sale, and import the Suggestions, including the right to sublicense such rights through multiple tiers, alone or in combination.

4.5 Government Rights. If you are using the Services on behalf of the government and these terms fail to meet the government's needs or are inconsistent in any respect with federal or state law, you will immediately discontinue your use of the Services (including any AWS Materials).

5. Representations and Warranties. You represent and warrant that (a) you and your End Users' use of the Services (including any use by your employees and personnel) will not violate this Access Policy; (b) you or your

licensors own all right, title, and interest in and to Your Materials; (c) Your Materials (including the use, development, design, production, advertising, or marketing of your Materials) or the combination of your Materials with other applications, content or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) your use of the Services will not cause harm to any End User.

6. Indemnification. Except to the extent prohibited by applicable state law, you will defend, indemnify, and hold harmless us, our licensors and each of our respective employees, officers, directors, and representatives from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to any third party claim concerning: (a) your or any End Users' use of the Services (including use by your employees and personnel); (b) Your Materials or the combination of Your Materials with other applications, content or processes, including any claim involving alleged infringement or misappropriation of third-party rights or the use, development, design, production, advertising or marketing of Your Materials; or (c) a dispute between you and any End User. If your ability to comply with the foregoing provision is limited to any extent by the absence of appropriations or government authorization, you will make good faith efforts to obtain sufficient appropriations or authorization for any liabilities arising under this Section 5.

7. Disclaimers. WE PROVIDE THE SERVICES ON AN "AS IS" BASIS TO PROVIDER. WE AND OUR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND TO YOU, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICES OR ANY THIRD PARTY MATERIALS, INCLUDING ANY WARRANTY THAT THE SERVICES OR THIRD PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY MATERIALS, INCLUDING YOUR MATERIALS OR THE THIRD PARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

8. Limitations of Liability. YOU MUST LOOK SOLELY TO PROVIDER AND YOUR AGREEMENT WITH THEM REGARDING ANY CLAIMS OR DAMAGES RELATED TO THE SERVICES. WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) SUSPENSION OF YOUR USE OF OR ACCESS TO THE SERVICES, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICES, OR, (III) ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON; OR (B) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR MATERIALS OR OTHER DATA THAT YOU OR ANY END USER SUBMITS OR USES IN CONNECTION WITH THE SERVICES (INCLUDING AS A RESULT OF YOUR OR ANY END USERS' ERRORS, ACTS OR OMISSIONS).

9. Miscellaneous.

9.1 Governing Law; Venue. Except to the extent prohibited by applicable state law, the laws of the State of Washington, without reference to conflict of law rules, govern this Access Policy and any dispute of any sort that might arise between you and us. You irrevocably consent to exclusive jurisdiction and venue of the federal courts located in King County, Washington with respect to any dispute arising in connection with the Services or this Access Policy. We may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of our or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply.

9.2 Entire Policy. This Access Policy is the final AWS policy governing your access to and use of the Services. It supersedes all prior or contemporaneous representations, understandings, agreements, or communications between you and us (if any), whether written or verbal, regarding the subject matter of this Access Policy. If the

terms of this document are inconsistent with the terms contained in your agreement with Provider, the terms contained in this document will control. We will not be bound by, and specifically object to, any term, condition or other provision which is different from or in addition to the provisions of this Access Policy (whether or not it would materially alter it) and which is submitted by you in any order, receipt, acceptance, confirmation, correspondence or other document.

9.3 Survival. The following provisions will survive any termination of your use of the Services: Sections 2.1, 4, 5, 6, 7, 8, 9 and 10.

10. Definitions.

“Acceptable Use Policy” means the policy currently available at <http://aws.amazon.com/aup>, as it may be updated by us from time to time.

“AWS Materials” means Materials we make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Materials does not include the Services.

“AWS Service Level Agreement” means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time.

“AWS Site” means <http://aws.amazon.com> and any successor or related site designated by us.

“Documentation” means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals, instructions and specifications for the Services currently located at <http://aws.amazon.com/documentation>, as such documentation may be updated by us from time to time.

“End User” means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Materials; or (b) otherwise accesses or uses the Services through you.

“Materials” means software (including machine images), data, text, audio, video, images or other content.

“Policies” means the Acceptable Use Policy, the Terms of Use, the Service Terms, all restrictions described in the AWS Materials and on the AWS Site, and any other policy or terms referenced in or incorporated into this Access Policy.

“Services” means, collectively or individually (as applicable), the web services made commercially available by us to Provider for use under this Access Policy, including (as applicable) those web services described in the Service Terms.

“Service Terms” means the rights and restrictions for particular Services located at <http://aws.amazon.com/serviceterms>, as they may be updated by us from time to time.

“Suggestions” means all suggested improvements to the Services or AWS Materials that you provide to us.

“Terms of Use” means the terms of use located at <http://aws.amazon.com/terms/>, as they may be updated by us from time to time.

“Third Party Materials” means Materials made available to you by any third party on the AWS Site or in conjunction with the Services.

“Your Materials” means Materials you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services or otherwise transfer, process, use or store in connection with the Services.



Exhibit 3. Applicable Terms and Conditions for Microsoft Azure.

Microsoft Cloud Agreement

This Microsoft Cloud Agreement is entered into between the entity you represent, or, if you do not designate an entity in connection with a Subscription purchase or renewal, you individually ("Customer"), and Microsoft Corporation ("Microsoft"). It consists of the terms and conditions below, Use Rights, SLA, and all documents referenced within those documents (together, the "agreement"). It is effective on the date that your Reseller provisions your Subscription. Key terms are defined in Section 10.

1. *Grants, rights and terms.*

All rights granted under this agreement are non-exclusive and non-transferable and apply as long as neither Customer nor any of its Affiliates is in material breach of this agreement.

- a. **Software.** Upon acceptance of each order, Microsoft grants Customer a limited right to use the Software in the quantities ordered.
 - (i) **Use Rights.** The Use Rights in effect when Customer orders Software will apply to Customer's use of the version of the Software that is current at the time. For future versions and new Software, the Use Rights in effect when those versions and Software are first released will apply. Changes Microsoft makes to the Use Rights for a particular version will not apply unless Customer chooses to have those changes apply.
 - (ii) **Temporary and perpetual licenses.** Licenses available on a subscription basis are temporary. For all other licenses, the right to use Software becomes perpetual upon payment in full.
- b. **Online Services.** Customer may use the Online Services as provided in this agreement.
 - (i) **Online Services Terms.** The Online Services Terms in effect when Customer orders or renews a subscription to an Online Service will apply for the applicable subscription term. For Online Services that are billed periodically based on consumption, the Online Services Terms current at the start of each billing period will apply to usage during that period.
 - (ii) **Suspension.** Microsoft may suspend use of an Online Service during Customer's violation of the Acceptable Use Policy or failure to respond to a claim of alleged infringement. Microsoft will give Customer notice before suspending an Online Service when reasonable.
 - (iii) **End Users.** Customer controls access by End Users, and is responsible for their use of the Product in accordance with this agreement. For example, Customer will ensure End Users comply with the Acceptable Use Policy.
 - (iv) **Customer Data.** Customer is solely responsible for the content of all Customer Data. Customer will secure and maintain all rights in Customer Data necessary for Microsoft to provide the Online Services to Customer without violating the rights of any third party or otherwise obligating Microsoft to Customer or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to Customer's use of the Product other than as expressly set forth in this agreement or as required by applicable law.
 - (v) **Responsibility for your accounts.** Customer is responsible for maintaining the confidentiality of any non-public authentication credentials associated with Customer's use of the Online Services. Customer must promptly notify customer support about any possible misuse of Customer's accounts or authentication credentials or any security incident related to the Online Services.

- c. **Reservation of rights.** Products are protected by copyright and other intellectual property rights laws and international treaties. Microsoft reserves all rights not expressly granted in this agreement. No rights will be granted or implied by waiver or estoppel. Rights to access or use Software on a device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.
- d. **Restrictions.** Customer may use the Product only in accordance with this agreement. Customer may not (and is not licensed to): (1) reverse engineer, decompile or disassemble any Product or Fix, or attempt to do so; (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (3) work around any technical limitations in a Product or Fix or restrictions in Product documentation. Customer may not disable, tamper with, or otherwise attempt to circumvent any billing mechanism that meters Customer's use of the Online Services. Except as expressly permitted in this agreement or Product documentation, Customer may not distribute, sublicense, rent, lease, lend, resell or transfer and Products, in whole or in part, or use them to offer hosting services to a third party.
- e. **Preview releases.** Microsoft may make Previews available. **Previews are provided "as-is," "with all faults," and "as-available," and are excluded from the SLA and all limited warranties provided in this agreement.** Previews may not be covered by customer support. Previews may be subject to reduced or different security, compliance, and privacy commitments, as further explained in the Online Services Terms and any additional notices provided with the Preview. Microsoft may change or discontinue Previews at any time without notice. Microsoft also may choose not to release a Preview into "General Availability."
- f. **Verifying compliance for Products.**
- (i) **Right to verify compliance.** Customer must keep records relating to all use and distribution of Products by Customer and its Affiliates. Microsoft has the right, at its expense, to verify compliance with the Products' license terms. Customer must promptly provide any information reasonably requested by the independent auditors retained by Microsoft in furtherance of the verification, including access to systems running the Products and evidence of licenses for Products that Customer hosts, sublicenses, or distributes to third parties. Customer agrees to complete Microsoft's self-audit process, which Microsoft may request as an alternative to a third party audit.
- (ii) **Remedies for non-compliance.** If verification or self-audit reveals any unlicensed use of Products, then within 30 days (1) Customer must order sufficient licenses to cover its use, and (2) if unlicensed use is 5% or more, Customer must reimburse Microsoft for the costs Microsoft incurred in verification and acquire the necessary additional licenses at 125% of the price, based on the then-current price last and customer price level. The unlicensed use percentage is based on the total number of licenses purchased for current use compared to the actual installed base. If there is no unlicensed use, Microsoft will not subject Customer to another verification for at least one year. By exercising the rights and procedures described above, Microsoft does not waive its rights to enforce this agreement or to protect its intellectual property by any other legal means.
- (iii) **Verification process.** Microsoft will notify Customer at least 30 days in advance of its intent to verify Customers' compliance with the license terms for the Products Customer and its Affiliates use or distribute. Microsoft will engage an independent auditor, which will be subject to a confidentiality obligation. Any information collected in the self-audit will be used solely for purposes of determining compliance. This verification will take place during normal business hours and in a manner that does not unreasonably interfere with Customer's operations.

2. **Subscriptions, ordering.**

- a. Choosing a Reseller.** Customer must choose and maintain a Reseller authorized within its region. If Microsoft or Reseller chooses to discontinue doing business with each other, Customer must choose a replacement Reseller or purchase a Subscription directly from Microsoft, which may require Customer to accept different terms.
- b. Available Subscription offers.** The Subscription offers available to Customer will be established by its Reseller and generally can be categorized as one or a combination of the following:
- (i) Online Services Commitment Offering.** Customer commits in advance to purchase a specific quantity of Online Services for use during a Term and to pay upfront or on a periodic basis for continued use of the Online Service.
 - (ii) Consumption Offering (also called Pay-As-You-Go).** Customer pays based on actual usage with no upfront commitment.
 - (iii) Limited Offering.** Customer receives a limited quantity of Online Services for a limited term without charge (for example, a free trial) or as part of another Microsoft offering (for example, MSDN). Provisions in this agreement with respect to the SLA and data retention may not apply.
 - (iv) Software Commitment Offering.** Customer commits in advance to purchase a specific quantity of Software for use during a Term and to pay upfront or on a periodic basis for continued use of the Software.
- c. Ordering.**
- (i)** Orders must be placed through Customer's designated Reseller. Customer may place orders for its Affiliates under this agreement and grant its Affiliates administrative rights to manage the Subscription, but, Affiliates may not place orders under this agreement. Customer also may assign the rights granted under Section 1.a and 1.b to a third party for use by that third party in Customer's internal business. If Customer grants any rights to Affiliates or third parties with respect to Software or Customer's Subscription, such Affiliates or third parties will be bound by this agreement and Customer agrees to be jointly and severally liable for any actions of such Affiliates or third parties related to their use of the Products.
 - (ii)** Customer's Reseller may permit Customer to modify the quantity of Online Services ordered during the Term of a Subscription. Additional quantities of Online Services added to a Subscription will expire at the end of that Subscription.
- d. Pricing and payment.** Prices for each Product and any terms and conditions for invoicing and payment will be established by Customer's Reseller.
- e. Renewal.**
- (i)** Upon renewal of a Subscription, Customer may be required to sign a new agreement, a supplemental agreement or an amendment to this agreement.
 - (ii)** Customer's Subscription will automatically renew unless Customer provides its Reseller with notice of its intent not to renew prior to the expiration of the Term.
- f. Eligibility for Academic, Government and Nonprofit versions.** Customer agrees that if it is purchasing an academic, government or nonprofit offer, Customer meets the respective eligibility requirements listed at the following sites:
- (i)** For academic offers, the requirements for educational institutions (including administrative offices or boards of education, public libraries, or public museums) listed at <http://go.microsoft.com/academic>;
 - (ii)** For government offers, the requirements listed at <http://go.microsoft.com/government>; and

(iii) For nonprofit offers, the requirements listed at <http://go.microsoft.com/nonprofit>.

Microsoft reserves the right to verify eligibility at any time and suspend the Online Service if the eligibility requirements are not met.

- g. Taxes.** The parties are not liable for any of the taxes of the other party that the other party is legally obligated to pay and which are incurred or arise in connection with or related to the transactions contemplated under this agreement, and all such taxes will be the financial responsibility of the party who is obligated by operation of law to pay such tax.

3. *Term, termination.*

- a. Agreement term and termination.** This agreement will remain in effect until the expiration or termination of Customer's Subscription, whichever is earliest. Customer may terminate this agreement at any time by contacting its Reseller. The expiration or termination of this agreement will only terminate Customer's right to place new orders for additional Products under this agreement.
- b. Termination for cause.** If either party breaches this Agreement, the other party may terminate the breached agreement (in whole or in part, including orders) upon notice. If the breach is curable within 30 days, then the terminating party must provide 30 days' notice to the breaching party and an opportunity to cure the breach.
- c. Cancel a Subscription.** Customer's Reseller will establish the terms and conditions, if any, upon which Customer may cancel a Subscription.

4. *Security, privacy, and data protection.*

- a. Reseller Administrator Access and Customer Data.** Customer acknowledges and agrees that (i) once Customer has chosen a Reseller, that Reseller will be the primary administrator of the Online Services for the Term and will have administrative privileges and access to Customer Data, however, Customer may request additional administrator privileges from its Reseller; (ii) Customer can, at its sole discretion and at any time during the Term, terminate its Reseller's administrative privileges; (iii) Reseller's privacy practices with respect to Customer Data or any services provided by Reseller are subject to the terms of Customer's agreement with its Reseller and may differ from Microsoft's privacy practices; and (iv) Reseller may collect, use, transfer, disclose, and otherwise process Customer Data, including personal data. Customer consents to Microsoft providing Reseller with Customer Data and information that Customer provides to Microsoft for purposes of ordering, provisioning and administering the Online Services.
- b.** Customer consents to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement. Customer may choose to provide personal information to Microsoft on behalf of third parties (including your contacts, resellers, distributors, administrators, and employees) as part of this agreement. Customer will obtain all required consents from third parties under applicable privacy and data protection laws before providing personal information to Microsoft.
- c.** Additional privacy and security details are in the Online Services Terms. The commitments made in the Online Services Terms only apply to the Online Services purchased under this agreement and not to any services or products provided by a Reseller.
- d.** As and to the extent required by law, Customer shall notify the individual users of the Online Services that their data may be processed for the purpose of disclosing it to law enforcement or other governmental authorities as directed by Reseller or as required by law, and Customer shall obtain the users' consent to the same.

- e. Customer appoints Reseller as its agent for purposes of interfacing with and providing instructions to Microsoft for purposes of this Section 4.

5. Warranties.

a. Limited warranty.

- (i) **Software.** Microsoft warrants that each version of the Software will perform substantially as described in the applicable Product documentation for one year from the date Customer is first licensed for that version. If it does not, and Customer notifies Microsoft within the warranty term, then Microsoft will, at its option, (1) return the price Customer paid for the Software license or (2) repair or replace the Software.
- (ii) **Online Services.** Microsoft warrants that each Online Service will perform in accordance with the applicable SLA during Customer's use. Customer's remedies for breach of this warranty are in the SLA.

The remedies above are Customer's sole remedies for breach of the warranties in this section. Customer waives any breach of warranty claims not made during the warranty period.

- b. **Exclusions.** The warranties in this agreement do not apply to problems caused by accident, abuse or use inconsistent with this agreement, including failure to meet minimum system requirements. These warranties do not apply to free or trial products, Previews, Limited Offerings, or to components of Products that Customer is permitted to redistribute.
- c. **Disclaimer.** Except for the limited warranties above, Microsoft provides no warranties or conditions for Products and disclaims any other express, implied, or statutory warranties for Products, including warranties of quality, title, non-infringement, merchantability and fitness for a particular purpose.

6. Defense of third party claims.

The parties will defend each other against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if the defending party is promptly notified in writing of the claim and has the right to control the defense and any settlement of it. The party being defended must provide the defending party with all requested assistance, information, and authority. The defending party will reimburse the other party for reasonable out-of-pocket expenses it incurs in providing assistance. This section describes the parties' sole remedies and entire liability for such claims.

- a. **By Microsoft.** Microsoft will defend Customer against any third-party claim to the extent it alleges that a Product or Fix made available by Microsoft for a fee and used within the scope of the license granted under this agreement (unmodified from the form provided by Microsoft and not combined with anything else), misappropriates a trade secret or directly infringes a patent, copyright, trademark or other proprietary right of a third party. If Microsoft is unable to resolve a claim of infringement under commercially reasonable terms, it may, as its option, either: (1) modify or replace the Product or fix with a functional equivalent; or (2) terminate Customer's license and refund any prepaid license fees (less depreciation on a five-year, straight-line basis) for perpetual licenses and any amount paid for Online Services for any usage period after the termination date. Microsoft will not be liable for any claims or damages due to Customer's continued use of a Product or Fix after being notified to stop due to a third-party claim.
- b. **By Customer.** To the extent permitted by applicable law, Customer will defend Microsoft against any third-party claim to the extent it alleges that: (1) any Customer Data or non-Microsoft software hosted in an Online Service by Microsoft on Customer's behalf

misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party; or (2) Customer's use of any Product or Fix, alone or in combination with anything else, violates the law or harms a third party.

7. *Limitation of liability.*

For each Product, each party's maximum, aggregate liability to the other under this agreement is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the applicable Products during the term of this agreement, subject to the following:

- a. Online Services.** For Online Services, Microsoft's maximum liability to Customer for any incident giving rise to a claim will not exceed the amount Customer paid for the Online Service during the 12 months before the incident; provided that in no event will Microsoft's aggregate liability for any Online Service exceed the amount paid for that Online Service during the Subscription.
- b. Free Products and distributable code.** For Products provided free of charge and code that Customer is authorized to redistribute to third parties without separate payment to Microsoft, Microsoft's liability is limited to direct damages finally awarded up to US\$5,000.
- c. Exclusions.** In no event will either party be liable for loss of revenue or indirect, special, incidental, consequential, punitive, or exemplary damages, or damages for loss of use, lost profits, revenues, business interruption, or loss of business information, however caused or on any theory of liability.
- d. Exceptions.** The limits of liability in this section apply to the fullest extent permitted by applicable law, but do not apply to: (1) the parties' obligations under section 6; or (2) violation of the other's intellectual property rights.

8. *Support.*

Customer's Reseller will provide details on support services available for Products purchased under this agreement.

9. *Miscellaneous.*

- a. Notices.** You must send notices by mail, return receipt requested, to the address below.

Notices should be sent to:

Microsoft Corporation
Volume Licensing Group
One Microsoft Way
Redmond, WA 98052
USA

Via Facsimile: (425) 936-7329

You agree to receive electronic notices from us, which will be sent by email to the account administrator(s) named for your Subscription. Notices are effective on the date on the return receipt or, for email, when sent. You are responsible for ensuring that the email address for the account administrator(s) named for your Subscription is accurate and current. Any email

notice that we send to that email address will be effective when sent, whether or not you actually receive the email.

- b. Assignment.** You may not assign this agreement either in whole or in part. Microsoft may transfer this agreement without your consent, but only to one of Microsoft's Affiliates. Any prohibited assignment is void.
- c. Severability.** If any part of this agreement is held unenforceable, the rest remains in full force and effect.
- d. Waiver.** Failure to enforce any provision of this agreement will not constitute a waiver.
- e. No agency.** This agreement does not create an agency, partnership, or joint venture.
- f. No third-party beneficiaries.** There are no third-party beneficiaries to this agreement.
- g. Use of contractors.** Microsoft may use contractors to perform services, but will be responsible for their performance, subject to the terms of this agreement.
- h. Microsoft as an independent contractor.** The parties are independent contractors. Customer and Microsoft each may develop products independently without using the other's confidential information.
- i. Agreement not exclusive.** Customer is free to enter into agreements to license, use or promote non-Microsoft products or services.
- j. Applicable law and venue.** This agreement is governed by Washington law, without regard to its conflict of laws principles, except that (i) if you are a U.S. Government entity, this agreement is governed by the laws of the United States, and (ii) if you are a state or local government entity in the United States, this agreement is governed by the laws of that state. Any action to enforce this agreement must be brought in the State of Washington. This choice of jurisdiction does not prevent either party from seeking injunctive relief in any appropriate jurisdiction with respect to violation of intellectual property rights.
- k. Entire agreement.** This agreement is the entire agreement concerning its subject matter and supersedes any prior or concurrent communications. In the case of a conflict between any documents in this agreement that is not expressly resolved in those documents, their terms will control in the following order of descending priority: (1) this agreement, (2) the Product Terms, (3) the Online Services Terms, and (4) any other documents in this agreement.
- l. Survival.** All provisions survive termination of this agreement except those requiring performance only during the term of the agreement.
- m. U.S. export jurisdiction.** Products are subject to U.S. export jurisdiction. Customer must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end-use and destination restrictions issued by U.S. and other governments related to Microsoft products, services, and technologies.
- n. Force majeure.** Neither party will be liable for any failure in performance due to causes beyond that party's reasonable control (such as fire, explosion, power blackout, earthquake, flood, severe storms, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism (including cyber terrorism), acts of God, acts or omissions of Internet traffic carriers, actions or omissions of regulatory or governmental bodies (including the passage of laws or regulations or other acts of government that impact the delivery of Online Services)). This Section will not, however, apply to your payment obligations under this agreement.
- o. Contracting authority.** If you are an individual accepting these terms on behalf of an entity, you represent that you have the legal authority to enter into this agreement on that entity's behalf.

10. Definitions.

Any reference in this agreement to “day” will be a calendar day.

“Acceptable Use Policy” is set forth in the Online Services Terms.

“Affiliate” means any legal entity that a party owns, that owns a party, or that is under common ownership with a party. “Ownership” means, for purposes of this definition, control of more than a 50% interest in an entity.

“Consumption Offering”, “Commitment Offering”, or “Limited Offering” describe categories of Subscription offers and are defined in Section 2.

“Customer Data” is defined in the Online Services Terms.

“End User” means any person you permit to access Customer Data hosted in the Online Services or otherwise use the Online Services.

“Fix” means a Product fix, modifications or enhancements, or their derivatives, that Microsoft either releases generally (such as Product service packs) or provides to Customer to address a specific issue.

“Licensing Site” means <http://www.microsoft.com/licensing/contracts> or a successor site.

“Non-Microsoft Product” is defined in the Online Services Terms.

“Online Services” means any of the Microsoft-hosted online services subscribed to by Customer under this agreement, including Microsoft Dynamics Online Services, Office 365 Services, Microsoft Azure Services, or Microsoft Intune Online Services.

“Online Services Terms” means the additional terms that apply to Customer’s use of Online Services published on the Licensing Site and updated from time to time.

“Previews” means preview, beta, or other pre-release version or feature of the Online Services or Software offered by Microsoft to obtain customer feedback.

“Product” means all products identified in the Product Terms, such as all Software, Online Services and other web-based services, including Previews.

“Product Terms” means the document that provides information about Microsoft Products and Professional Services available through volume licensing. The Product Terms document is published on the Licensing Site and is updated from time to time.

“Reseller” means an entity authorized by Microsoft to resell Software licenses and Online Service Subscriptions under this program and engaged by you to provide assistance with your Subscription.

“SLA” means Service Level Agreement, which specifies the minimum service level for the Online Services and is published on the Licensing Site.

“Software” means licensed copies of Microsoft software identified on the Product Terms. Software does not include Online Services, but Software may be a part of an Online Service.

“Subscription” means an enrollment for Online Services for a defined Term as established by your Reseller.

“Term” means the duration of a Subscription (e.g., 30 days or 12 months).

“Use Rights” means the use rights or terms of service for each Product published on the Licensing Site and updated from time to time. The Use Rights supersede the terms of any end user license agreement that accompanies a Product. The Use Rights for Software are published by Microsoft in the Product Terms. The Use Rights for Online Services are published in the Online Services Terms.



Online Services Terms January 1, 2017

Table of Contents

INTRODUCTION	3	ONLINE SERVICE SPECIFIC TERMS	15
PRIOR VERSIONS	3	MICROSOFT AZURE SERVICES	15
CLARIFICATIONS AND SUMMARY OF CHANGES	3	MICROSOFT COGNITIVE SERVICES	16
Microsoft Cognitive Services	3	MICROSOFT AZURE PLANS	17
Microsoft Translator	3	AZURE ACTIVE DIRECTORY BASIC	17
Office 365 Advanced Compliance	3	AZURE ACTIVE DIRECTORY PREMIUM	17
Office 365 Advanced eDiscovery	3	AZURE INFORMATION PROTECTION PREMIUM	17
Yammer	3	MICROSOFT DYNAMICS 365 SERVICES	17
GENERAL TERMS	4	OFFICE 365 SERVICES	19
Definitions	4	EXCHANGE ONLINE	19
Online Services Terms Updates	4	OFFICE 365 APPLICATIONS	20
Online Services Changes and Availability	4	MICROSOFT MYANALYTICS	21
Data Retention	4	OFFICE 365 ADVANCED COMPLIANCE	21
Use of Software with the Online Service	4	OFFICE ONLINE	21
Non-Microsoft Products	5	ONEDRIVE FOR BUSINESS	21
Acceptable Use Policy	5	PROJECT ONLINE	21
Technical Limitations	5	SHAREPOINT ONLINE	22
Compliance with Laws	5	SKYPE FOR BUSINESS ONLINE	22
Import/Export Services	6	SKYPE FOR BUSINESS ONLINE PSTN SERVICES	23
Electronic Notices	6	OTHER ONLINE SERVICES	23
License Reassignment	6	BING MAPS ENTERPRISE PLATFORM AND BING MAPS MOBILE ASSET	
Font Components	6	MANAGEMENT PLATFORM	23
Competitive Benchmarking	6	BUSINESS APPLICATION PLATFORM	25
Multiplexing	6	MICROSOFT INTUNE	25
PRIVACY AND SECURITY TERMS	7	MICROSOFT LEARNING	25
GENERAL PRIVACY AND SECURITY TERMS	7	MINECRAFT: EDUCATION EDITION	26
Scope	7	OFFICE 365 DEVELOPER	26
Use of Customer Data	7	WINDOWS DESKTOP OPERATING SYSTEM	26
Disclosure of Customer Data	7	ATTACHMENT 1 – NOTICES	27
Educational Institutions	7	BING MAPS	27
HIPAA Business Associate	7	PROFESSIONAL SERVICES	27
Security	8	NOTICE ABOUT AZURE MEDIA SERVICES H.265/HEVC ENCODING	28
Security Incident Notification	8	NOTICE ABOUT H.264/AVC VISUAL STANDARD, VC-1 VIDEO STANDARD,	
Location of Data Processing	8	MPEG-4 PART VISUAL STANDARD AND MPEG-2 VIDEO STANDARD	28
Preview Releases	8	ATTACHMENT 2 – SUBSCRIPTION LICENSE SUITES	29
Use of Subcontractors	8	ATTACHMENT 3 – THE STANDARD CONTRACTUAL CLAUSES	
How to Contact Microsoft	8	(PROCESSORS)	30
DATA PROCESSING TERMS	9		
Location of Customer Data at Rest	10		
Privacy	10		
Additional European Terms	10		
Security	12		

Introduction

Beginning July 1, 2014 these Online Services Terms (OST) replace the Online Services Use Rights (OLSUR). The OST contains terms that apply to Customer's use of Online Services. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products (as defined below), as well as other products and services from Microsoft.

Most Online Services offer a Service Level Agreement (SLA). For more information regarding the Online Services SLAs, please refer to <http://microsoft.com/licensing/contracts>.

Prior Versions

The OST provides terms for Online Services that are currently available. For earlier versions Customer may refer to <http://go.microsoft.com/?linkid=9840733> or contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes

Additions	Deletions
Microsoft Cognitive Services	Microsoft Translator
Office 365 Advanced Compliance	Office 365 Advanced eDiscovery
	Yammer

Privacy and Security Terms

Scope: The General Privacy and Security Terms do not apply to the Microsoft Cognitive Services. Among the most important differences is that Microsoft may retain Customer Data sent to the Microsoft Cognitive Services indefinitely to improve Microsoft products and services. Refer to the [Microsoft Cognitive Services](#) section for details.

Data Processing Terms

[Online Services Table](#): Microsoft Booking and Microsoft Planner have been added to the Office 365 Services section.
[Location of Customer Data at Rest](#): Project Online data has been added to the Office 365 Services section.

Online Service Specific Terms

[Microsoft Azure Services](#): Information related to Microsoft Translator is included with the Microsoft Cognitive Services entry.
[Office 365 Services](#): Office 365 Advanced eDiscovery has been renamed Office 365 Advanced Compliance. Yammer was removed as standalone entry and information related to External Users use of external network functionality was added to the Office 365 Services header section.

[Table of Contents / General Terms](#)

General Terms

Customer may use the Online Services and related software as expressly permitted in Customer's volume licensing agreement. Microsoft reserves all other rights. Customer must acquire and assign the appropriate subscription licenses required for its use of each Online Service. Each user that accesses the Online Service must be assigned a User SL or access the Online Service only through a device that has been assigned a Device SL, unless specified otherwise in the [Online Service-specific Terms, Attachment 2](#) describes SL Suites that also fulfill requirements for User SLs. Customer has no right to use an Online Service after the SL for that Online Service ends.

Definitions

If any of the terms below are not defined in Customer's volume licensing agreement, they have the definitions below.

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service.

"External User" means a user of an Online Service that is not an employee, onsite contractor, or onsite agent of Customer or its Affiliates.

"Instance" means an image of software that is created by executing the software's setup or install procedure or by duplicating such an image.

"Licensed Device" means the single physical hardware system to which a license is assigned. For purposes of this definition, a hardware partition or blade is considered to be a separate device.

"Non-Microsoft Product" means any third-party-branded software, data, service, website or product.

"Online Service" means a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement, including any service identified in the Online Services section of the Product Terms. The Product Terms is located at <http://go.microsoft.com/?linkid=9839207>.

"Operating System Environment" (OSE) means all or part of an operating system Instance, or all or part of a virtual (or otherwise emulated) operating system Instance, that enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and Instances of applications, if any, configured to run on all or part of that operating system Instance. There are two types of OSEs, physical and virtual. A physical hardware system can have one physical OSE and/or one or more virtual OSEs. The operating system Instance used to run hardware virtualization software or to provide hardware virtualization services is considered part of the physical OSE.

"SL" means subscription license.

Online Services Terms Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current OST will apply and will not change during Customer's subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the OST that apply to Customer's use of those new features, supplements or related software.

Online Services Changes and Availability

Microsoft may make commercially reasonable changes to each Online Service from time to time. Microsoft may terminate an Online Service in any country where Microsoft is subject to a government regulation, obligation or other requirement that is not generally applicable to businesses operating there. Availability, functionality, and language versions for each Online Service may vary by country. For information on availability, Customer may refer to www.microsoft.com/online/international-availability.aspx.

Data Retention

At all times during the term of Customer's subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data as described in this section.

Use of Software with the Online Service

Customer may need to install certain Microsoft software in order to use the Online Service. If so, the following terms apply:

Microsoft Software License Terms

Customer may install and use the software only for use with the Online Service. The [Online Service-specific Terms](#) may limit the number of copies of the software Customer may use or the number of devices on which Customer may use it. Customer's right to use the software begins

when the Online Service is activated and ends when Customer's right to use the Online Service ends. Customer must uninstall the software when Customer's right to use it ends. Microsoft may disable it at that time.

Validation, Automatic Updates, and Collection for Software

Microsoft may automatically check the version of any of its software. Devices on which the software is installed may periodically provide information to enable Microsoft to verify that the software is properly licensed. This information includes the software version, the end user's user account, product ID information, a machine ID, and the internet protocol address of the device. If the software is not properly licensed, its functionality will be affected. Customer may only obtain updates or upgrades for the software from Microsoft or authorized sources. By using the software, Customer consents to the transmission of the information described in this section. Microsoft may recommend or download to Customer's devices updates or supplements to this software, with or without notice. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications) ("Apps"). The Apps may collect data about the use and performance of the Apps, which may be transmitted to Microsoft and used for the purposes described in this OST.

Third-party Software Components

The software may contain third party software components. Unless otherwise disclosed in that software, Microsoft, not the third party, licenses these components to Customer under Microsoft's license terms and notices.

Non-Microsoft Products

Microsoft may make Non-Microsoft Products available to Customer through Customer's use of the Online Services (such as through a store or gallery, or as search results). If Customer installs or uses any Non-Microsoft Product with an Online Service, Customer may not do so in any way that would subject Microsoft's intellectual property or technology to obligations beyond those expressly included in Customer's volume licensing agreement. For Customer's convenience, Microsoft may include charges for the Non-Microsoft Product as part of Customer's bill for Online Services. Microsoft, however, assumes no responsibility or liability whatsoever for the Non-Microsoft Product. Customer is solely responsible for any Non-Microsoft Product that it installs or uses with an Online Service.

Acceptable Use Policy

Neither Customer, nor those that access an Online Service through Customer, may use an Online Service:

- in a way prohibited by law, regulation, governmental order or decree;
- to violate the rights of others;
- to try to gain unauthorized access to or disrupt any service, device, data, account or network;
- to spam or distribute malware;
- in a way that could harm the Online Service or impair anyone else's use of it; or
- in any application or situation where failure of the Online Service could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage.

Violation of the terms in this section may result in suspension of the Online Service. Microsoft will suspend the Online Service only to the extent reasonably necessary. Unless Microsoft believes an immediate suspension is required, Microsoft will provide reasonable notice before suspending an Online Service.

Technical Limitations

Customer must comply with, and may not work around, any technical limitations in an Online Service that only allow Customer to use it in certain ways. Customer may not download or otherwise remove copies of software or source code from an Online Service except as explicitly authorized.

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to privacy, biometric data, data protection and confidentiality of communications. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application), and for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation. Customer is responsible for responding to any request from a third party regarding Customer's use of an Online Service, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Import/Export Services

Customer's use of any Import/Export Service is conditioned upon its compliance with all instructions provided by Microsoft regarding the preparation, treatment and shipment of physical media containing its data ("storage media"). Customer is solely responsible for ensuring the storage media and data are provided in compliance with all laws and regulations. Microsoft has no duty with respect to the storage media and no liability for lost, damaged or destroyed storage media. All storage media shipped to Microsoft must be shipped DAP Microsoft DCS Data Center (INCOTERMS 2010). Storage media shipped to Customer will be shipped DAP Customer Dock (INCOTERMS 2010).

Electronic Notices

Microsoft may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

License Reassignment

Most, but not all, SLs may be reassigned. Except as permitted in this paragraph or in the [Online Service-specific Terms](#), Customer may not reassign an SL on a short-term basis (i.e., within 90 days of the last assignment). Customer may reassign an SL on a short-term basis to cover a user's absence or the unavailability of a device that is out of service. Reassignment of an SL for any other purpose must be permanent. When Customer reassigns an SL from one device or user to another, Customer must block access and remove any related software from the former device or from the former user's device.

Font Components

While Customer uses an Online Service, Customer may use the fonts installed by that Online Service to display and print content. Customer may only embed fonts in content as permitted by the embedding restrictions in the fonts and temporarily download them to a printer or other output device to print content.

Competitive Benchmarking

If Customer offers a service competitive to an Online Service, by using the Online Service, Customer agrees to waive any restrictions on competitive use and benchmark testing in the terms governing its competitive service. If Customer does not intend to waive such restrictions in its terms of use, Customer is not allowed to use the Online Service.

Multiplexing

Hardware or software that Customer uses to pool connections; reroute information; reduce the number of devices or users that directly access or use the Online Service (or related software); or reduce the number of OSEs, devices or users the Online Service directly manages (sometimes referred to as "multiplexing" or "pooling") does not reduce the number of licenses of any type (including SLs) that Customer needs.

[Table of Contents](#) / [General Terms](#)

Privacy and Security Terms

This section of the Online Services Terms has two parts:

- General Privacy and Security Terms, which apply to all Online Services; and
- Data Processing Terms, which are additional commitments for certain Online Services.

General Privacy and Security Terms

Scope

The terms in this section apply to all Online Services except Bing Maps Enterprise Platform, Bing Maps Mobile Asset Management Platform, and Microsoft Cognitive Services, which are governed by the privacy and/or security terms referenced below in the applicable [Online Service-specific Terms](#).

Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Disclosure of Customer Data

Microsoft will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law.

Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third party request for Customer Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will not provide any third party: (a) direct, indirect, blanket or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) apply, Microsoft acknowledges that for the purposes of the OST, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Microsoft's possession as may be required under applicable law.

HIPAA Business Associate

If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of Customer's volume licensing agreement includes execution of the HIPAA Business Associate Agreement ("BAA"), the full text of which identifies the Online Services to which it applies and is available at <http://aka.ms/BAA>. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer's volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out;
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the opt out applies.

Security

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Location of Data Processing

Except as described elsewhere in the OST, Customer Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. Customer appoints Microsoft to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Online Services. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland. In addition to Microsoft's commitments under the Standard Contractual Clauses and other model contracts, Microsoft is certified to the EU-U.S. Privacy Shield Framework and the commitments it entails.

Preview Releases

Microsoft may offer preview, beta or other pre-release features, data center locations, and services ("Previews") for optional evaluation. Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise provided, Previews are not included in the SLA for the corresponding Online Service.

Use of Subcontractors

Microsoft may hire subcontractors to provide services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the OST.

How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at <http://go.microsoft.com/?linkid=9846224>. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

Microsoft Ireland Operations, Ltd.

Attn: Data Protection
Carmenhall Road
Sandyford, Dublin 18, Ireland

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Data Processing Terms

The Data Processing Terms (DPT) include the terms in this section.

The Data Processing Terms also include the “Standard Contractual Clauses,” pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU Data Protection Directive.

The Standard Contractual Clauses are in [Attachment 3](#). In addition,

- Execution of the volume licensing agreement includes execution of [Attachment 3](#), which is countersigned by Microsoft Corporation;
- The terms in Customer’s volume licensing agreement, including the DPT, constitute a data processing agreement under which Microsoft is the data processor; and
- The DPT control over any inconsistent or conflicting provision in Customer’s volume licensing agreement and, for each subscription, will remain in full force and effect until all of the related Customer Data is deleted from Microsoft’s systems in accordance with the DPT.

Customer may opt out of the “Standard Contractual Clauses” or the Data Processing Terms in their entirety. To opt out, Customer must send the following information to Microsoft in a written notice (under terms of the Customer’s volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out;
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the Opt Out applies;
- if opting out of the entire DPT, a statement that Customer (or Affiliate) opts out of the entirety of the Data Processing Terms; and
- if opting out of only the Standard Contractual Clauses, a statement that Customer (or Affiliate) opts out of the Standard Contractual Clauses only.

In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

In the DPT, the term “Online Services” applies only to the services in the table below, excluding any Previews, and “Customer Data” includes only Customer Data that is provided through use of those Online Services.

Online Services	
Microsoft Dynamics 365 Core Services	The following services, each as a standalone service or as included in a Dynamics 365 branded plan or application: Microsoft Dynamics 365 for Customer Service, Microsoft Dynamics 365 for Field Service, Microsoft Dynamics 365 for Project Service Automation, Microsoft Dynamics 365 for Sales, and Microsoft Social Engagement. Microsoft Dynamics 365 Core Services do not include (1) Microsoft Dynamics 365 for Operations or Microsoft Dynamics 365 for Financials; (2) Microsoft Dynamics 365 Services for supported devices or software, which includes but is not limited to Microsoft Dynamics 365 for apps, tablets and/or phones; or (3) except as expressly defined in the licensing terms for the corresponding service, any other separately-branded service made available with or connected to Microsoft Dynamics 365 Core Services.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, Office 365 Advanced Threat Protection, SharePoint Online, OneDrive for Business, Microsoft Planner, Project Online, Skype for Business Online, Sway, Office Online, Microsoft MyAnalytics, Customer Lockbox, Microsoft Bookings, and Yammer Enterprise. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft’s control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded “for Office 365.”
Microsoft Azure Core Services	Active Directory, API Management, App Services (API Apps, Mobile Apps, Web Apps, Automation, Backup, Batch, BizTalk Services, Cloud Services, DocumentDB, Event Hubs, Express Route, HDInsight, Key Vault, Load Balancer, Machine Learning, Management Portal, Media Services, Multi-Factor Authentication, Notification Hub, Operational Insights, Redis Cache, Rights Management Service, Scheduler, Service Bus, Site Recovery, SQL Database, Storage, StorSimple, Stream Analytics, Traffic Manager, Virtual Machines, Virtual Network, Visual Studio Team Services, and Workflow Manager.
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.
Microsoft Power BI Services	The cloud service portion of Microsoft Power BI offered as a standalone service or as included in an Office 365-branded plan or suite, but excluding data catalog functionality, the Power BI mobile applications, or Power BI Desktop.

Location of Customer Data at Rest

Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows:

- **Office 365 Services.** If Customer provisions its tenant in Australia, Canada, the European Union, India, Japan or the United States (each of the foregoing a Geo), Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, and Project Online data, and (3) files uploaded to OneDrive for Business.
- **Microsoft Intune Online Services.** When Customer provisions a tenant account, Customer selects an available Geo where Customer Data at rest will be stored. Microsoft will not transfer the Customer Data outside of Customer's selected Geo except as noted in the "Data Location" section of the Microsoft Intune Trust Center.
- **Microsoft Power BI Services.** If Customer provisions its tenant in Australia, the European Union, or the United States, Microsoft will store Microsoft Power BI Customer Data at rest only within that Geo.
- **Microsoft Azure Core Services.** If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo. Certain services may not enable Customer to configure deployment in a particular Geo or outside the United States and may store backups in other locations, as detailed in the Microsoft Azure Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing Services in general release).
- **Microsoft Dynamics 365 Core Services.** Except for Microsoft Social Engagement, if Customer provisions its instance in the United States or the EU, Microsoft will store Customer Data at rest in any of these Geos, limited to the entities managed by Microsoft Dynamics 365 Core Services. Certain entities may not be configured to be stored in any particular Geo or outside the United States and may be replicated in other locations as detailed in the Microsoft Dynamics 365 Trust Center.

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Privacy

- **Customer Data Deletion or Return.** No more than 180 days after expiration or termination of Customer's use of an Online Service, Microsoft will disable the account and delete Customer Data from the account.
- **Transfer of Customer Data.** Unless Customer has opted out of the Standard Contractual Clauses, all transfers of Customer Data out of the European Union, European Economic Area, and Switzerland shall be governed by the Standard Contractual Clauses. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland.
- **Microsoft Personnel.** Microsoft personnel will not process Customer Data without authorization from Customer. Microsoft personnel are obligated to maintain the security and secrecy of any Customer Data as provided in the DPT and this obligation continues even after their engagements end.
- **Subcontractor Transfer.** Microsoft may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Microsoft provides a website that lists subcontractors authorized to access Customer Data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorizing any new subcontractor to access Customer Data, Microsoft will update the website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent Customer invoices.

Additional European Terms.

These Additional European Terms apply only if Customer has end users in the European Economic Area ("EEA") or Switzerland.

- **End Users in EEA or Switzerland.** Terms used in the DPT that are not specifically defined will have the meaning in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Data Protection Directive").
- **Intent of the Parties.** For the Online Services, Microsoft is a data processor (or sub-processor) acting on Customer's behalf. As data processor (or sub-processor), Microsoft will only act upon Customer's instructions. The OST and Customer's volume licensing agreement (including the terms and conditions incorporated by reference therein), along with Customer's use and configuration of features in the Online Services, are Customer's complete and final instructions to Microsoft for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's volume licensing agreement.
- **Duration and Object of Data Processing.** The duration of data processing shall be for the term designated under Customer's volume licensing agreement. The objective of the data processing is the performance of the Online Services.

- **Scope and Purpose of Data Processing.** The scope and purpose of processing of Customer Data, including any personal data included in the Customer Data, is described in the DPT and Customer's volume licensing agreement.
- **Customer Data Access.** For the term designated under Customer's volume licensing agreement Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

Security

- **General Practices.** Microsoft has implemented and will maintain and follow for the Online Services the following security measures, which, in conjunction with the security commitments in the OST, are Microsoft's only responsibility with respect to the security of Customer Data.

Domain	Practices
Organization of Information Security	Security Ownership. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. Security Roles and Responsibilities. Microsoft personnel with access to Customer Data are subject to confidentiality obligations. Risk Management Program. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	Asset Inventory. Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. Asset Handling - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.
Human Resources Security	Security Training. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.
Physical and Environmental Security	Physical Access to Facilities. Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. Physical Access to Components. Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain. Protection from Disruptions. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. Component Disposal. Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	Operational Policy. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. Data Recovery Procedures - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. Malicious Software. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. Data Beyond Boundaries - Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Microsoft restricts access to Customer Data in media leaving its facilities. Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	Access Policy. Microsoft maintains a record of security privileges of individuals having access to Customer Data. Access Authorization - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. Least Privilege

Domain	Practices
	- Technical support personnel are only permitted to have access to Customer Data when needed. - Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function. Integrity and Confidentiality - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. Authentication - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. Network Design. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	Incident Response Process - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made without unreasonable delay and, in any event, within 30 calendar days. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. Service Monitoring. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located. - Microsoft’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

Online Services Information Security Policy

Each Online Service follows a written data security policy (“Information Security Policy”) that complies with the control standards and frameworks shown in the table below.

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes	Yes
Microsoft Dynamics 365 Core Services	Yes	Yes	Yes	Yes*	Yes*
Microsoft Azure Core Services	Yes	Yes	Yes	Varies**	Varies**
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Power BI Services	Yes	Yes	Yes	No	No

*Does not include Microsoft Social Engagement.

**Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate a standard or framework in the table above, unless it is no longer used in the industry and it is replaced with a successor (if any). Azure Government Services meet a separate set of control standards and frameworks, as detailed on the Microsoft Azure Trust Center.

Subject to non-disclosure obligations, Microsoft will make each Information Security Policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

Customer is solely responsible for reviewing each Information Security Policy and making an independent determination as to whether it meets Customer's requirements.

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses.

Microsoft Audits of Online Services

For each Online Service, Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Microsoft's Confidential Information. The Microsoft Audit Report will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report so that Customer can verify Microsoft's compliance with the security obligations under the DPT. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

If the Standard Contractual Clauses apply, then (1) Customer agrees to exercise its audit right by instructing Microsoft to execute the audit as described in this section of the DPT, and (2) if Customer desires to change this instruction, then Customer has the right to do so as set forth in the Standard Contractual Clauses, which shall be requested in writing.

If the Standard Contractual Clauses apply, then nothing in this section of the DPT varies or modifies the Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. Microsoft Corporation is an intended third-party beneficiary of this section.

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Online Service Specific Terms

If an Online Service is not listed below, it does not have any Online Service-specific terms.

Microsoft Azure Services

Notices

The Bing Maps, Professional Services, Azure Media Services H.265/HEV Encoding, and H.264/AVC Visual Standard, VC-1 Video Standard, and MPEG-4 Part 2 Visual Standard and MPEG-2 Video Standard Notices in [Attachment 1](#) apply.

Service Level Agreement

Refer to <http://azure.microsoft.com/support/legal/sla/>.

Definitions

“Azure Government Services” means one or more of the services or features Microsoft makes available to Customer as Government Community Cloud Services in the “US Gov” regions identified at <http://azure.microsoft.com/en-us/regions/#services>.

“Customer Solution” means an application or any set of applications that adds primary and significant functionality to the Microsoft Azure Services and that is not primarily a substitute for the Microsoft Azure Services.

“Microsoft Azure Services” means one or more of the Microsoft services and features identified at <http://azure.microsoft.com/services/>, except where identified as licensed separately.

“Microsoft Translator” means Translator API Text Translation and/or Translator API Speech Translation offered by Microsoft as a cloud based automatic translation service.

Limitations

Customer may not

- resell or redistribute the Microsoft Azure Services, or
- allow multiple users to directly or indirectly access any Microsoft Azure Service feature that is made available on a per user basis (e.g., Active Directory Premium). Specific reassignment terms applicable to a Microsoft Azure Service feature may be provided in supplemental documentation for that feature.

Retirement of Services or Features

Microsoft will provide Customer with 12 months’ notice before removing any material feature or functionality or discontinuing a service, unless security, legal or system performance considerations require an expedited removal. This does not apply to Previews

Data Retention after Expiration or Termination

The expiration or termination of Customer’s Online Service subscription will not change Customer’s obligation to pay for hosting of Customer Data during any Extended Term.

Hosting Exception

Customer may create and maintain a Customer Solution and, despite anything to the contrary in Customer’s volume licensing agreement, combine Microsoft Azure Services with Customer Data owned or licensed by Customer or a third party, to create a Customer Solution using the Microsoft Azure Service and the Customer Data together. Customer may permit third parties to access and use the Microsoft Azure Services in connection with the use of that Customer Solution. Customer is responsible for that use and for ensuring that these terms and the terms and conditions of Customer’s volume licensing agreement are met by that use.

Use of Software within Microsoft Azure

For Microsoft software available within a Microsoft Azure Service, Microsoft grants Customer a limited license to use the software only within the Microsoft Azure Service.

Data Center Availability

Usage of data centers in certain regions may be restricted to Customers located in or near that region. For information on service availability by region, please refer to <http://azure.microsoft.com/en-us/regions>.

Sharing

The Microsoft Azure Services may provide the ability to share a Customer Solution and/or Customer Data with other Azure users and communities, or other third parties. If Customer chooses to engage in such sharing, Customer agrees that it is giving a license to all authorized users, including the rights to use, modify, and repost its Customer Solution and/or the Customer Data, and Customer is allowing Microsoft to make them available to such users in a manner and location of its choosing.

Marketplace

Microsoft Azure enables Customer to access or purchase Non-Microsoft Products through features such as the Microsoft Azure Marketplace and the Virtual Machine Gallery, subject to separate terms available at <http://azure.microsoft.com/en-us/support/legal/store-terms>.

Microsoft Cognitive Services

Microsoft Cognitive Services Privacy

The Microsoft Privacy Statement located at <https://go.microsoft.com/fwlink/?LinkId=521839> applies to Customer's use of Microsoft Cognitive Services, except that this Microsoft Cognitive Services section controls to the extent it conflicts with the Microsoft Privacy Statement.

Use of Cognitive Services Data.

Customer is solely responsible for the content of all Customer Data it sends to the Cognitive Services ("Cognitive Services Data").

Microsoft may process Cognitive Services Data solely to: (i) provide Cognitive Services to Customer; and (ii) improve Microsoft products and services. Solely for such processing, Microsoft may collect, retain, use, reproduce, and create derivative works of, Cognitive Services Data and Customer grants Microsoft a limited nonexclusive irrevocable worldwide license to do so. Customer will secure and maintain all rights necessary for Microsoft to process Cognitive Services Data as described in this paragraph without violating the rights of any third party or otherwise obligating Microsoft to Customer or to any third party.

Where Cognitive Services Data includes personal data, Customer will obtain sufficient consent for such processing by Microsoft from the data subjects (or from their parents or guardians as required by applicable law).

Microsoft is committed to helping protect data subjects who may be identifiable from Cognitive Services Data that Microsoft retains. Microsoft has implemented business and technical measures designed to help de-identify some retained Cognitive Services Data.

This Use of Cognitive Services Data section will survive termination or expiration of Customer's volume licensing agreement. As between the parties, Customer retains all right, title and interest in and to Cognitive Services Data. Microsoft acquires no rights in Cognitive Services Data, other than the rights Customer grants to Microsoft in this Use of Cognitive Services Data section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Cognitive Services Data Retention

Unless stated in documentation for a service, Cognitive Services are not designed to store Customer Data on Customer's behalf.

Application of General Privacy and Security Terms

Only the following sections of the General Privacy and Security Terms apply to the Cognitive Services: Location of Data Processing, Preview Releases, Use of Subcontractors, How to Contact Microsoft

Attribution

When using the Microsoft Cognitive Services (except the Search APIs (defined below)), Customer will provide reasonably prominent attribution. The attribution should read "using Microsoft Cognitive Services" and include a hyperlink to <http://go.microsoft.com/fwlink/?LinkID=829046>.

Precedence

This Microsoft Cognitive Services section controls to the extent there is any conflict with other parts of the OST.

Bing APIs Limit on Customer use of service output

Customer may not use any data from the Bing-branded APIs for the purpose of developing or offering any comparable machine-learning based service.

Bing Search APIs Use and Display Requirements

Customer must comply with use and display requirements for the Bing Web Search, Image Search, Video Search and News Search APIs, Bing Spell Check, and Bing Autosuggest (collectively, the “Search APIs”), which are available here <https://aka.ms/r1j7jq>. Customer must use results it obtains through the Search APIs only in Internet Search Experiences (as defined in the use and display requirements) and must not cache or copy results. The results Customer obtains through the Search APIs are not Products, Fixes, or Services Deliverables.

Translator API

Attribution:

When displaying automatic translations performed by Microsoft Translator, Customer will provide reasonably prominent notice that the text has been automatically translated by Microsoft Translator.

Limit on Customer use of service output:

Customer may not use any data from Microsoft Translator for the purpose of developing or offering any comparable machine-learning based service.

[Table of Contents](#) / [General Terms](#)

Microsoft Azure Plans

Notices

The Bing Maps Notices in [Attachment 1](#) apply.

Subscription License Suites

In addition to User SLs, refer to [Attachment 2](#) for other SLs that fulfill requirements for Azure Active Directory Premium, Azure Information Protection, and Microsoft Intune.

Azure Active Directory Basic

Customer may, using Single Sign-On, pre-integrate up to 10 SAAS Applications/Custom Applications per User SL. All Microsoft as well as third party applications count towards this application limit.

[Table of Contents](#) / [General Terms](#)

Azure Active Directory Premium

Customer may, using Single Sign-On, pre-integrate SaaS Applications/Custom Applications. Customer may not copy or distribute any data set (or any portion of a data set) included in the Microsoft Identity Manager software that is included with a Microsoft Azure Active Directory Premium (P1 and P2) User SL.

[Table of Contents](#) / [General Terms](#)

Azure Information Protection Premium

Notices

The Bing Maps Notices in [Attachment 1](#) applies. Any deployment services provided to Customer are subject to the Professional Services Notice in [Attachment 1](#).

[Table of Contents](#) / [General Terms](#)

Microsoft Dynamics 365 Services

Microsoft Dynamics 365 Case Management, Enterprise Edition
Microsoft Dynamics 365 Customer Service, Enterprise Edition
Microsoft Dynamics 365 Field Services, Enterprise Edition
Microsoft Dynamics 365 Financials, Business Edition
Microsoft Dynamics 365 Operations, Enterprise Edition

Microsoft Dynamics 365 Project Service Automation, Enterprise Edition
Microsoft Dynamics 365 Sales, Enterprise Edition
Microsoft Dynamics 365 Team Members, Business Edition
Microsoft Dynamics 365 Team Members, Enterprise Edition

Notices

The Bing Maps and Professional Services Notices in [Attachment 1](#) apply. Any onboarding, migration, or deployment services provided to Customer as subject to the Professional Services Notice in [Attachment 1](#).

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Subscription License Suites

In addition to User SLs, refer to [Attachment 2](#) for other offerings that fulfill SL requirements.

External Users

External Users of Microsoft Dynamics 365 Services do not need a SL to access the Online Service. This exemption does not apply to contractors or agents of Customer or its Affiliate.

Microsoft Dynamics 365 for Operations

Customer may modify Microsoft Dynamics 365 for Operations to allow extension of its functionality, but only for Customer's internal use purposes.

Server Use Rights for Dynamics 365 User SLs, From SA User SLs and Add-on User SLs

Customer with active Microsoft Dynamics 365 Services subscriptions may:

- install and use any number of copies of the Microsoft Dynamics Server software on any server;
- allow users or devices licensed with Microsoft Dynamics CRM CALs and Microsoft Dynamics AX CALs to access Microsoft Dynamics Server software provided with Microsoft Dynamics 365 subscriptions;
- receive and use updates related to government tax and regulatory requirements on Microsoft Dynamics Server software;
- modify or create derivative works of plug-ins, runtime, and other components identified in printed or online documentation and use those derivative works, but only with the Microsoft Dynamics Server software and only for Customer's internal purposes; and
- run passive fail-over instances of Microsoft Dynamics Server software for temporary support.

Microsoft Social Engagement

Service Level Agreement

There is no SLA for Microsoft Social Engagement.

Social Content Obtained through Microsoft Social Engagement

Social Content is publicly-available content collected from social media networks (such as Twitter, Facebook and YouTube) and data indexing or data aggregation services in response to Customer's search queries executed in Microsoft Social Engagement. Social Content is not Customer Data. Customer Data used in configuring or initiating search queries executed on Customer's behalf may be shared with third parties for purposes of collecting Social Content. Customer may use Social Content for its internal business purposes only. Microsoft reserves the right to:

- store Social Content in a database commingled with content aggregated from other sources by other licensees;
- access, edit or delete Social Content in response to a request from a social media network, data indexing or data aggregation service, Social Content owner or a takedown request under the Digital Millennium Copyright Act;
- instruct Customer to edit or delete Social Content if Customer exports Social Content; and
- delete or restrict further access to Social Content after the Online Service has been terminated or expires.

[Table of Contents](#) / [General Terms](#)

Office 365 Services

Notices

The Bing Maps Notices in [Attachment 1](#) apply. Any onboarding, migration, or deployment services provided to Customer are subject to the Professional Services Notice in [Attachment 1](#).

Core Features for Office 365 Services

During the term of Customer's subscription, the Office 365 Services will substantially conform to the Core Features description provided (if any) in the Office 365 service-specific sections below, subject to Product restrictions or external factors (such as the recipient, message rate, message size and mailbox size limits for e-mail; default or Customer-imposed data retention policies; search limits; storage limits; Customer or end user configurations; and meeting capacity limits). Microsoft may permanently eliminate a functionality specified below only if it provides Customer a reasonable alternative functionality.

Administration Portal

Customer will be able to add and remove end users and domains, manage licenses, and create groups through the Microsoft Online Services Portal or its successor site.

Subscription License Suites

In addition to User SLs, refer to [Attachment 2](#) for other SLs that fulfill requirements for Office 365 Services.

Microsoft Teams

Notice: The H.264/MPEG-4 AVC Notice in [Attachment 1](#) applies to all Office 365 Services that include Microsoft Teams.

Yammer

For Office 365 Services that include Yammer, External Users invited to Yammer via external network functionality do not need User SLs.

Exchange Online

Office 365 Advanced Threat Protection
Data Loss Prevention
Exchange Online Archiving for Exchange Online

Exchange Online Archiving for Exchange Server
Exchange Online Kiosk
Exchange Online (Plan 1 and Plan 2)

Core Features for Office 365 Services – Exchange Online

Exchange Online or its successor service will have the following [Core Features](#) capabilities:

Emails

An end user will be able to send email messages, receive email messages that originate from within and outside of Customer's organization, and access the end user's mailbox.

Mobile and Web Browser Access

Through the Microsoft Exchange ActiveSync protocol or a successor protocol or technology, Exchange Online will enable an end user to send and receive emails and update and view calendars from a mobile device that adequately supports such a protocol or technology. An end user will be able to send email messages, receive email messages that originate from within and outside of Customer's organization, and access the end user's mailbox, all from within a compatible web browser.

Retention Policies

Customer will be able to establish archive and deletion policies for email messages.

Deleted Item and Mailbox Recovery

Customer will be able to recover the contents of a deleted non-shared mailbox and an end user will be able to recover an item that has been deleted from one of the end user's email folders.

Multi-Mailbox Search

Customer will be able to search for content across multiple mailboxes within its organization.

Calendar

An end user will be able to view a calendar and schedule appointments, meetings, and automatic replies to incoming email messages.

Contacts

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Privacy and Security Terms](#)

[Online Service – specific Terms](#)

[Attachments](#)

Through an Exchange Online-provided user interface, Customer will be able to create and manage distribution groups and an organization-wide directory of mail-enabled end users, distribution groups, and external contacts.

Core Features for Office 365 Services – Exchange Online Archiving

Exchange Online Archiving or its successor service will have the following [Core Features](#) capabilities:

Storage

Customer will be able to allow an end user to store email messages.

Retention Policies

Customer will be able to establish archive and deletion policies for email messages distinct from policies that an end user can apply to the end user's own mailbox.

Deleted Item and Mailbox Recovery

Customer, through Office 365 support services, will be able to recover a deleted archive mailbox, and an end user will be able to recover an item that has been deleted from one of the end user's email folders in the end user's archive.

Multi-Mailbox Search

Customer will be able to search for content across multiple mailboxes within its organization.

Legal Hold

Customer will be able to place a "legal hold" on an end user's primary mailbox and archive mailbox to preserve the content of those mailboxes.

Archiving

Archiving may be used for messaging storage only with Exchange Online Plans 1 and 2.

Archiving for Exchange Server

Users licensed for Exchange Server 2013 Standard Client Access License may access the Exchange Server 2013 Enterprise Client Access License features necessary to support use of Exchange Online Archiving for Exchange Server.

Exchange Online Plan 2 from Exchange Hosted Archive Migration

Exchange Online Plan 2 is a successor Online Service to Exchange Hosted Archive. If Customer renews from Exchange Hosted Archive into Exchange Online Plan 2 and has not yet migrated to Exchange Online Plan 2, Customer's licensed users may continue to use the Exchange Hosted Archive service subject to the terms of the March 2011 Product Use Rights until the earlier of Customer's migration to Exchange Online Plan 2 or the expiration of Customer's Exchange Online Plan 2 User SLs. The Product Use Rights is located at <http://go.microsoft.com/?linkid=9839206>.

Data Loss Prevention Device License

If Customer is licensed for Data Loss Prevention by Device, all users of the Licensed Device are licensed for the Online Service.

Service Level Agreement

There is no SLA for Office 365 Advanced Threat Protection.

[Table of Contents](#) / [General Terms](#)

Office 365 Applications

Office 365 Business
Office 365 ProPlus

Visio Pro for Office 365

Service Level Agreement

There is no SLA for Visio Pro for Office 365.

Installation and Use Rights

Each user to whom Customer assigns a User SL must have a Microsoft Account in order to use the software provided with the subscription. These users:

- may activate the software provided with the SL on up to five concurrent OSEs for local or remote use;
- may also install and use the software, with shared computer activation, on a shared device, a network server, or on shared servers with a qualified cloud partner. A list of qualified cloud partners and additional deployment requirements is available at www.office.com/sca. For the

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

purpose of this use right “network server” means a physical hardware server solely dedicated to Customer use. This shared computer activation provision does not apply to Customers license for Office 365 Business; and

- must connect each device upon which user has installed the software to the Internet at least once every 30 days or the functionality of the software may be affected.

The following terms apply only to Office 365 Business and Office 365 ProPlus

Smartphone and Tablet Devices

Each user to whom Customer assigns a User SL may also activate Microsoft Office Mobile software to use on up to five smartphones and five tablets.

The following terms apply only to Office 365 ProPlus

Office Home & Student 2013 RT Commercial Use

Each User SL for Office 365 ProPlus modifies the user’s right to use the software under a separately acquired Office Home & Student 2013 RT license by waiving the prohibition against commercial use. Except for this allowance for commercial use of the software, all use is subject to the terms and use rights provided with the Office Home & Student 2013 RT License.

Office Online Server

For each Office 365 ProPlus subscription, Customer may install any number of copies of Office Online Server on any Server dedicated to Customer’s use. Each Office 365 ProPlus user may use the Office Online Server software. This provision does not apply to Customers that license this Product under the Microsoft Online Subscription Agreement or other Microsoft agreement that cover Online Services only.

Subscription License Suites

In addition to Office 365 ProPlus User SLs, Customer may fulfill the SL requirement for this Product by purchasing a Suite SL (refer [Attachment 2](#)).

[Table of Contents](#) / [General Terms](#)

Microsoft MyAnalytics

Service Level Agreement

There is no SLA for Microsoft MyAnalytics.

[Table of Contents](#) / [General Terms](#)

Office 365 Advanced Compliance

Service Level Agreement

There is no SLA for Office 365 Advanced Compliance.

[Table of Contents](#) / [General Terms](#)

Office Online

Core Features for Office 365 Services

Office Online or its successor service will have the following [Core Features](#) capabilities:

An end user will be able to create, view, and edit documents in Microsoft Word, Excel, PowerPoint, and OneNote file types that are supported by Office Online or its successor service.

External Users

External Users invited to site collections via Share-by-Mail functionality do not need User SLs with Office Online.

[Table of Contents](#) / [General Terms](#)

OneDrive for Business

External Users

External Users invited to site collections via Share-by-Mail functionality do not need User SLs with OneDrive for Business.

[Table of Contents](#) / [General Terms](#)

Project Online

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Installation and Use Rights for Project application

Each user to whom Customer assigns a Project Online Professional or Project Online Premium User SL must have a Microsoft Account in order to use the software provided with the subscription. These users:

- may activate the software provided with the SL on up to five concurrent OSEs for local or remote use;
- may also install and use the software, with shared computer activation, on a shared device, a network server, or on shared servers with a qualified cloud partner. A list of qualified cloud partners and additional deployment requirements is available at www.office.com/sca. For the purpose of this use right “network server” means a physical hardware server solely dedicated to Customer use; and
- must connect each device upon which user has installed the software to the Internet at least once every 30 days or the functionality of the software may be affected.

[Table of Contents](#) / [General Terms](#)

SharePoint Online

Core Features for Office 365 Services

SharePoint Online or its successor service will have the following [Core Features](#) capabilities:

Collaboration Sites

An end user will be able to create a web browser-accessible site through which the end user can upload and share content and manage who has permission to access that site.

Storage

Customer will be able to set storage capacity limits for a site created by an end user.

External Users

External Users invited to site collections via Share-by-Mail functionality do not need User SLs with SharePoint Online Kiosk, Plan 1 and Plan 2.

Storage Add-on SLs

Office 365 Extra File Storage is required for each gigabyte of storage in excess of the storage provided with User SLs for SharePoint Online Plans 1 and 2.

[Table of Contents](#) / [General Terms](#)

Skype for Business Online

Notices

The H.264/MPEG-4 AVC and/or VC-1 Notices in [Attachment 1](#) apply.

Core Features for Office 365 Services

Skype for Business Online Plan 1 and Plan 2 or their successor services will have the following [Core Features](#) capabilities:

Instant Messaging

An end user will be able to transfer a text message to another end user in real time over an Internet Protocol network.

Presence

An end user will be able to set and display the end user’s availability and view another end user’s availability.

Online Meetings

An end user will be able to conduct an Internet-based meeting that has audio and video conferencing functionality with other end users.

External Users and users not authenticated by Skype for Business Online

User SLs are not required for External Users and users not authenticated by the Skype for Business Online service.

Skype for Business Online PSTN Services

Skype for Business Online PSTN Calling
Skype for Business Online PSTN Conferencing

Skype for Business PSTN Consumption

PSTN Services

Skype for Business Online PSTN Services ("PSTN Services") enable users to communicate with others via the worldwide voice telephone network known generally as the Public Switched Telephone Network. PSTN Services are provided by the Microsoft Affiliate authorized to provide them. Pricing for PSTN Services may include applicable taxes and fees. All included taxes and fees are disclosed on the Volume Licensing site (<http://go.microsoft.com/fwlink/?LinkId=690247>)

Important Information About Emergency Services

Customer must notify each user of Skype for Business Online PSTN Calling that Emergency Services operate differently than on traditional telephone services in the following ways: (i) Skype for Business may not know the actual location of an Emergency Services caller, which could result in the call being routed to the wrong Emergency Services call center and/or emergency services being dispatched to the wrong location; (ii) if the user's device has no power, is experiencing a power outage or, for any reason, cannot otherwise access the Internet, the user cannot make an Emergency Services call through Skype for Business PSTN Calling services; and (iii) although Skype for Business Online PSTN Calling services can be used anywhere in the world where an Internet connection is available, users should not make an Emergency Services call from a location outside their home country because the call likely will not be routed to the appropriate call center in that location.

Limitations on use

Customer may not exceed the usage limitations for the applicable PSTN Service subscription plan. Doing so may result in suspension of the services. Microsoft will provide reasonable notice before suspending PSTN Services, and customer will be able to make emergency calls during any period of suspension.

Other Online Services

Bing Maps Enterprise Platform and Bing Maps Mobile Asset Management Platform

Service SLs

A Service SL is required to access the services via the Bing Maps Enterprise Platform or Bing Maps Mobile Asset Management Platform. Each Service SL must be purchased with at least one of the following qualifying Add-On SLs:

- For the Bing Maps Enterprise Platform Service SL, either:
 - Bing Maps Public Website Usage Add-on SL, which is available for a specified number of billable transactions for use on a website that is available publicly without restriction,
 - Bing Maps Internal Website Usage Add-on SL, which is available for a specified number of billable transactions for use on an internal website (e.g., intranet) on a private network,
 - Bing Maps Known User Add-on SL, or
 - Bing Maps Light Known User Add-on SL.
- For the Bing Maps Mobile Asset Management Platform Service SL; for each Asset either:
 - Bing Maps Asset Management for North America Add-on SL
 - Bing Maps Asset Management for Europe Add-on SL, or
 - Bing Maps Asset Management for Rest of World Add-on SL

Qualifying Bing Maps Mobile Asset Management Platform Service SL Add-on SLs

For the Bing Maps Mobile Asset Management Platform, an Add-on SL is required for each tracked Asset whose GPS or other sensor based position can be monitored, displayed, reverse geocoded or used to perform calculations using Bing Maps Mobile Asset Management Platform. "Asset" is defined as any vehicle, device or other mobile object. These Add-on SLs are for a specified number of tracked Assets.

Authenticated Users

Users that are authenticated by Customer's programs that access Bing Maps Enterprise Platform and Bing Maps Mobile Asset Management Platform must have a SL.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Bing Maps APIs

Customer may use all Bing Maps APIs in accordance with the Microsoft Bing Maps Platform API Terms of Use and Bing Maps Platform SDKs, including any successors thereto, located at <https://aka.ms/bingmapsplatformapistou> and <https://aka.ms/bingmapsplatformsdks>.

Bing Maps Privacy

The Bing Privacy Statement and privacy terms in the Microsoft Bing Maps Platform API Terms of Use located at: <https://go.microsoft.com/fwlink/?LinkId=521839> apply to Customer's use of the Bing Maps Services.

[Table of Contents](#) / [General Terms](#)

Business Application Platform

Microsoft Power BI Pro

Notices

The Bing Maps Notices in [Attachment 1](#) apply.

[Table of Contents](#) / [General Terms](#)

Microsoft Intune

Microsoft Intune (per user)

Microsoft Intune Add-on for System Center Configuration

Windows Intune Add-on for System Center Configuration Manager and System Center Endpoint Protection (per user)
("Microsoft Intune Add-On")

Notices

Any deployment services provided to Customer are subject to the Professional Services Notice in [Attachment 1](#).

Manage Devices

Each user to whom Customer assigns a User SL may access and use the Online Service and related software (including System Center software) to manage up to fifteen devices.

Storage Add-on SL

A Storage Add-on SL is required for each gigabyte of storage in excess of the storage provided with the base subscription.

Windows Software Components in System Center Software

The System Center software includes one or more of the following Windows Software Components: Microsoft .NET Framework, Microsoft Data Access Components, Powershell software and certain .dlls related to Microsoft Build, Windows Identity Foundation, Windows Library for JavaScript, Debghelp.dll, and Web Deploy technologies. The license terms governing use of the Windows Software Components are in the Windows 8.1 Pro and Enterprise section of the Product Terms. The Product Terms is located at <http://go.microsoft.com/?linkid=9839206>.

SQL Server Technology and Benchmarking

The Software included with the Online Service includes SQL Server-branded components other than a SQL Server Database. Those components are licensed to Customer under the terms of their respective licenses, which can be found in the installation directory or unified installer of the software. Customer must obtain Microsoft's prior written approval to disclose to a third party the results of any benchmark test of these components or the software that includes them.

[Table of Contents](#) / [General Terms](#)

Microsoft Learning

Microsoft Learning E-Reference Library

Any person that has valid access to Customer's computer or internal network may copy and use the documentation for Customer's internal reference purposes. Documentation does not include electronic books.

Microsoft Learning Imagine Academy Service SL

A Service SL is required for each Location that accesses or uses any Microsoft Imagine Academy service or benefit. Location is defined as a physical site with staff under the same administrator, such as a principal, in a single building or group of buildings located on the same campus.

[Table of Contents](#)

→ [Introduction](#)

→ [General Terms](#)

→ [Privacy and Security Terms](#)

→ [Online Service – specific Terms](#)

→ [Attachments](#)

Microsoft Learning Imagine Academy Program Guidelines

The Imagine Academy program guidelines, located at <http://www.microsoft.com/itacademy>, apply to Customer's use of the Microsoft Learning Imagine Academy and its benefits.

Microsoft Learning Imagine Academy Program Benefits Provided by Third-Party

Program benefits may only be used by a licensed institution's faculty, staff and students currently enrolled in the licensed institution.

[Table of Contents](#) / [General Terms](#)

Minecraft: Education Edition

Notices

The Bing Maps Notices in [Attachment 1](#) apply.

[Table of Contents](#) / [General Terms](#)

Office 365 Developer

No Production Use of Office 365 Developer

Each user to whom Customer assigns a User SL may use the Online Service to design, develop, and test Customer's applications to make them available for Customer's Office 365 Online Services, on-premises deployments or for the Microsoft Office Store. The Online Service is not licensed for production use.

Office 365 Developer End Users

Customer's end users do not need a SL to access Office 365 Developer to perform acceptance tests or provide feedback on Customer programs.

[Table of Contents](#) / [General Terms](#)

Windows Desktop Operating System

Data Retention

The Windows Defender Advanced Threat Protection portion of the product does not contain extractable Customer Data therefore the Customer Data extraction terms in the OST do not apply.

[Table of Contents](#) / [General Terms](#)

Attachment 1 – Notices

Bing Maps

The Online Service or its included software includes use of Bing Maps. Any content provided through Bing Maps, including geocodes, can only be used within the product through which the content is provided. Customer's use of Bing Maps is governed by the Bing Maps End User Terms of Use available at go.microsoft.com/fwlink?id=9710837 and the Bing Maps Privacy Statement available at go.microsoft.com/fwlink/?LinkID=248686.

[Table of Contents](#) / [General Terms](#)

Professional Services

Customer may be eligible for Microsoft customer support and consulting services related to this Online Service. These services are "Professional Services" under Customer's volume licensing agreement. If Customer's volume licensing agreement covers Online Services only (and does not define Professional Services), then these services are provided subject to the "Professional Services Terms" below.

The Professional Services to which this Notice applies are not Online Services, and the rest of the Online Services Terms, as well as any data processing amendment or HIPAA Business Associate Agreement signed by the parties, do not apply. Any information provided to Microsoft in connection with these Professional Services is protected under the confidentiality terms of Customer's volume licensing agreement.

Additional terms may apply to these Professional Services, but only to the extent those terms don't conflict with this Notice.

Professional Services Terms

Definition

Any services to which this notice applies are defined, collectively, as "Professional Services".

Obligations of the Parties

Microsoft warrants that all Professional Services will be performed with professional care and skill. If Microsoft fails to do so and Customer notifies Microsoft within 90 days of the date of performance, then Microsoft will either re-perform the Professional Services or return the price paid for them as Customer's sole remedy for breach of the Professional Services warranty.

Customer will perform its applicable responsibilities and obligations to support Microsoft's performance of the Professional Services, as specified in the description of each Professional Service.

Limitation of Liability

To the extent permitted by applicable law, each party's total liability for all claims relating to Professional Services will be limited to the amounts Customer was required to pay for the Professional Services or the limitation of liability for the Online Service with which the Professional Services are offered, whichever is greater. **In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, including loss of use, loss of profits, or interruption of business, however caused or on any theory of liability in relation to the Professional Services. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations; or (2) violation of the other party's intellectual property rights.**

Fixes

"Fixes" are Product fixes, modifications or enhancements, or their derivatives, that Microsoft either releases generally (such as service packs) or that Microsoft provides to Customer to address a specific issue. Each Fix, is licensed under the same terms as the Product to which it applies. If a Fix is not provided for a specific Product, any use terms Microsoft provides with the Fix will apply.

Pre-Existing Work

"Pre-Existing Work" means any computer code or non-code based written materials developed or otherwise obtained independent of Customer's volume licensing agreement. All rights in Pre-Existing Work shall remain the sole property of the party providing the Pre-Existing Work. Each party may use, reproduce and modify the other party's Pre-Existing Work only as needed to perform obligations related to Professional Services.

Services Deliverables

"Services Deliverables" means any computer code or materials other than Products or Fixes that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services. Microsoft grants Customer a non-exclusive, non-transferable, perpetual license to reproduce, use, and modify the Services Deliverables solely for Customer's internal business purposes, subject to the terms and conditions in Customer's volume licensing agreement.

Non-Microsoft Technology

Customer is solely responsible for any non-Microsoft software or technology that it installs or uses with the Online Services, Fixes, or Services Deliverables.

Affiliates' Rights

Customer may sublicense the rights to use Services Deliverables to its Affiliates, but Customer's Affiliates may not sublicense these rights. Customer is liable for ensuring its Affiliates' compliance with the terms of this Notice and Customer's volume licensing agreement.

Government Customers.

If Customer is a government entity, then the following terms apply to any Professional Services provided at no charge to Customer. Microsoft waives any and all entitlement to compensation from Customer for the Professional Services. In compliance with applicable laws and regulations, Microsoft and Customer acknowledge that the Professional Services are for the sole benefit and use of Customer and not provided for the personal use or benefit of any individual government employee.

[Table of Contents](#) / [General Terms](#)

Notice about Azure Media Services H.265/HEVC Encoding

Customer must obtain its own patent license(s) from any third party H.265/HEVC patent pools or rights holders before using Azure Media Services to encode or decode H.265/HEVC media.

[Table of Contents](#) / [General Terms](#)

Notice about H.264/AVC Visual Standard, VC-1 Video Standard, MPEG-4 Part Visual Standard and MPEG-2 Video Standard

This software may include H.264/AVC, VC-1, MPEG-4 Part 2, and MPEG-2 visual compression technology. MPEG LA, L.L.C. requires this notice: THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, THE MPEG-4 PART 2 AND MPEG-2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE (VIDEO STANDARDS) AND/OR (ii) DECODE AVC, VC-1, MPEG-4 PART 2 AND MPEG-2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. REFER TO www.mpegla.com.

For clarification purposes, this notice does not limit or inhibit the use of the software for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of content compliant with the VIDEO STANDARDS technologies for distribution to third parties.

[Table of Contents](#) / [General Terms](#)

Attachment 2 – Subscription License Suites

Online Services may be available for purchase as Suites of Online Services. If, in the table below, a cell is shaded blue in an Online Service's row, the Suite SL for the column the cell is in fulfills the SL requirements for the cell's Online Services.

Online Service	Office 365 Enterprise ^{1,3}				Office 365 Government					Office 365 Education		Office 365 Business Essentials	Office 365 Business Premium	Enterprise Mobility + Security		Secure Productive Enterprise ²	Dynamics 365 Enterprise Edition	
	K1	E1	E3	E5	K1	E1	E3	E4	E5	Edu	E5			E3	E5		Plan 1	Plan 2
Exchange Online																		
Exchange Online Kiosk																		
Exchange Online Plan 1																		
Exchange Online Plan 2																		
SharePoint Online																		
SharePoint Online Kiosk																		
SharePoint Online Plan 1																		
SharePoint Online Plan 2																		
Skype for Business Online																		
Skype for Business Online Plan 1																		
Skype for Business Online Plan 2																		
Skype for Business Online Cloud PBX																		
Skype for Business Online PSTN Conf.																		
OneDrive for Business																		
Office Online																		
Office 365 Business																		
Office 365 ProPlus																		
Office 365 Customer Lockbox																		
Microsoft MyAnalytics																		
Office 365 Advanced Compliance																		
Office 365 Advanced Security Management																		
Microsoft Power BI Pro																		
Office 365 Advanced Threat Protection																		
Microsoft Intune																		
Azure Info Protection Premium Plan 1																		
Azure Info Protection Premium Plan 2																		
Azure Active Directory Premium Plan 1																		
Azure Active Directory Premium Plan 2																		
Cloud App Security																		
Microsoft Dynamics 365 for Customer Service																		
Microsoft Dynamics 365 for Field Service																		
Microsoft Dynamics 365 for Operations																		
Microsoft Dynamics 365 for Project Service Automation																		
Microsoft Dynamics 365 for Sales																		
Microsoft Flow																		
Microsoft PowerApps																		

¹ Add-on Suite SLs that include "without ProPlus" in the title do not include rights to Office 365 ProPlus.

² In addition to the Online Services above, the Secure Productive Enterprise fulfills the SL requirement for Windows SA per User as described in the Product Terms.

³ Inclusion of Skype for Business Online PSTN Conferencing with Office 365 Enterprise E5 is dependent on regional availability.

Attachment 3 – The Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Microsoft Corporation (as data importer, whose signature appears below), each a “party,” together “the parties,” have agreed on the following Contractual Clauses (the “Clauses” or “Standard Contractual Clauses”) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law.

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter: Customer is the data exporter. The data exporter is a user of Online Services as defined in the section of the OST entitled "Data Processing Terms."

Data importer: The data importer is MICROSOFT CORPORATION, a global producer of software and services.

Data subjects: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer.

Categories of data: The personal data transferred includes e-mail, documents and other data in an electronic form in the context of the Online Services.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the applicable volume licensing agreement between data exporter and the Microsoft entity to which these Standard Contractual Clauses are annexed ("Microsoft"). The objective of the data processing is the performance of Online Services.

b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the DPT. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities.

c. Customer Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf.

d. Data Exporter's Instructions. For Online Services, data importer will only act upon data exporter's instructions as conveyed by Microsoft.

e. Customer Data Deletion or Return. Upon expiration or termination of data exporter's use of Online Services, it may extract Customer Data and data importer will delete Customer Data, each in accordance with the OST applicable to the agreement.

Subcontractors: The data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Personnel. Data importer's personnel will not process Customer Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.

2. Data Privacy Contact. The data privacy officer of the data importer can be reached at the following address:

Microsoft Corporation

Attn: Chief Privacy Officer

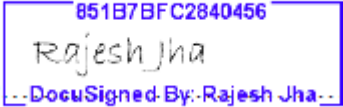
1 Microsoft Way

Redmond, WA 98052 USA

3. Technical and Organization Measures. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data, as defined in the DPT, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the DPT are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signature of Microsoft Corporation appears on the following page.

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2 on behalf of the data importer:

Signature  Rajesh Jha, Corporate Vice President
Microsoft Corporation
One Microsoft Way, Redmond WA, USA 98052

Product Terms January 1, 2017

Table of Contents

INTRODUCTION	4	VISUAL STUDIO	36
ABOUT THIS DOCUMENT	4	VISUAL STUDIO TEAM FOUNDATION SERVER	38
WHAT THIS DOCUMENT CONTAINS	4	WINDOWS	39
HOW TO NAVIGATE A PRODUCT ENTRY	4	WINDOWS DESKTOP OPERATING SYSTEM	39
CLARIFICATIONS AND SUMMARY OF CHANGES TO THIS DOCUMENT	5	WINDOWS SERVER	45
LICENSE TERMS	7	WINDOWS MULTIPoint SERVER	45
UNIVERSAL LICENSE TERMS	7	WINDOWS SERVER	46
LICENSE MODEL TERMS	9	ONLINE SERVICES	49
DESKTOP APPLICATIONS	9	ONLINE SERVICES REGIONAL AVAILABILITY	49
DESKTOP OPERATING SYSTEMS	10	ONLINE SERVICES PURCHASING RULES	49
PER CORE/CAL	10	ONLINE SERVICES RENEWAL	49
SERVER/CAL	10	MICROSOFT AZURE SERVICES	49
PER CORE	11	MICROSOFT AZURE SERVICES	51
MANAGEMENT SERVERS	11	MICROSOFT AZURE PLANS	51
SPECIALTY SERVERS	12	SECURE PRODUCTIVE ENTERPRISE	53
DEVELOPER TOOLS	12	ENTERPRISE MOBILITY + SECURITY (PLAN)	54
SOFTWARE	13	MICROSOFT DYNAMICS 365 SERVICES	55
ADVANCED THREAT ANALYTICS	13	OFFICE 365 SERVICES	57
BIZTALK	13	OFFICE 365 APPLICATIONS	57
CAL SUITES	14	OFFICE 365 SUITES	59
CORE INFRASTRUCTURE SERVER (CIS) SUITE	16	OFFICE 365 ADVANCED SECURITY MANAGEMENT	61
FOREFRONT	17	OFFICE 365 CUSTOMER LOCKBOX	61
MICROSOFT DYNAMICS	18	MICROSOFT MYANALYTICS	62
MICROSOFT DYNAMICS 365 ON-PREMISES	18	OFFICE 365 ADVANCED COMPLIANCE	62
MICROSOFT DYNAMICS AX	20	EXCHANGE ONLINE	62
MICROSOFT IDENTITY MANAGER	21	ONEDRIVE FOR BUSINESS	63
OFFICE APPLICATIONS	22	PROJECT ONLINE	63
OFFICE DESKTOP APPLICATIONS	22	SHAREPOINT ONLINE	64
OFFICE FOR MAC	23	SKYPE FOR BUSINESS ONLINE	64
OFFICE SERVERS	24	OTHER ONLINE SERVICES	65
EXCHANGE SERVER	24	BING MAPS	65
PROJECT SERVER	25	BUSINESS APPLICATION PLATFORM	66
SHAREPOINT SERVER	26	MICROSOFT INTUNE	66
SKYPE FOR BUSINESS SERVER	27	MICROSOFT LEARNING	66
R SERVER	28	MICROSOFT TRANSLATOR	67
SQL SERVER	28	MINECRAFT: EDUCATION EDITION	67
SYSTEM CENTER	30	GLOSSARY	69
SYSTEM CENTER SERVER	30	ATTRIBUTES	69
SYSTEM CENTER CONFIGURATION MANAGER	31	CELL VALUES	70
SYSTEM CENTER DATA PROTECTION MANAGER	32	COLUMN HEADINGS	70
SYSTEM CENTER ENDPOINT PROTECTION	33	DEFINITIONS	71
SYSTEM CENTER OPERATIONS MANAGER	33	APPENDIX A – CAL/ML EQUIVALENT LICENSES	73
SYSTEM CENTER ORCHESTRATOR	34	APPENDIX B – SOFTWARE ASSURANCE	74
SYSTEM CENTER SERVICE MANAGER	35	PURCHASING SOFTWARE ASSURANCE	74
VIRTUAL DESKTOP INFRASTRUCTURE (VDI) SUITE	36	RENEWING SOFTWARE ASSURANCE	74
VISUAL STUDIO	36		

MIGRATION LICENSE FOR DISCONTINUED OR END-OF-LIFE PRODUCTS..... 75

SOFTWARE ASSURANCE BENEFITS 75

APPENDIX C – PROFESSIONAL SERVICES.....86

MICROSOFT PREMIER SUPPORT OFFERINGS 86

MICROSOFT DIGITAL ADVISORY SERVICES OFFERINGS..... 86

SALES PRODUCTIVITY ACCELERATOR OFFERINGS 87

APPENDIX D – PROGRAM AGREEMENT SUPPLEMENTAL TERMS...88

SUPPLEMENTAL TERMS FOR SELECT PLUS PROGRAM 88

DEFINITION OF MANAGEMENT FOR QUALIFIED DEVICES..... 88

ONLINE SERVICES IN THE OPEN PROGRAMS..... 88

SUPPLEMENTAL TERMS FOR PROFESSIONAL SERVICES – LEGACY AGREEMENTS . 88

APPENDIX E – PROMOTIONS.....90

AZURE COMPUTE CAPACITY PROMOTION 90

NEW CUSTOMER AZURE MONETARY COMMITMENT OFFER..... 90

APPENDIX F - STORAGE ARRAY TERMS.....91

AVAILABILITY 91

SHIPMENT AND TITLE 91

STORAGE ARRAY SOFTWARE 91

LIMITED HARDWARE WARRANTY 91

INDEMNIFICATION. DEFENSE OF THIRD PARTY CLAIMS 92

LIMITATION OF LIABILITY 92

U.S. EXPORT CONTROL LAWS 92

COLLECTION OF DIAGNOSTIC INFORMATION 92

GOVERNMENT USE 92

INDEX 93

Introduction

About this Document

Beginning July 1, 2015, the Product Terms replaces both the Product List and the Product Use Rights (PUR) documents. All references to the Product List and PUR in Customer's volume licensing agreements refer to the applicable sections of the Product Terms. The Product Terms describe the availability of Products and Professional Services through the Microsoft Volume Licensing Programs (previously conveyed through the Product List), as well as the use rights for Software Products (previously conveyed through the PUR). Terms of service for the Online Services referenced in this document are published in the Online Services Terms (OST) at <http://go.microsoft.com/?linkid=9840733>.

Products listed in the Product Terms are available as of the date on the Product Terms [Cover Page](#). Earlier versions of the Product Terms are available on <http://go.microsoft.com/?linkid=9839207>, including earlier versions of the Product List and PUR documents. Information on discontinued Microsoft products and services is available on <http://www.microsoftvolumelicensing.com>. Customers should contact their reseller or Microsoft account manager for information pertaining to regional availability of Microsoft products and Professional Services.

What this Document contains

The Product Terms includes the following sections:

- [Introduction](#), which includes a list of recent changes.
- [License Terms](#), which list the Universal License Terms and License Model Terms that apply to Software Products.
- [Software Products](#), which list all Software Product Entries.
- [Online Services Products](#), which list all Online Services Product Entries.
- [Glossary](#), which defines Attributes, Cell Values, Column Headings and other capitalized terms used in the Product Terms.
- The following appendices:
 - [Appendix A – CAL/ML Equivalent Licenses Table](#), which identifies CAL suites and Online Services subscription Licenses available that provide access to Server Products.
 - [Appendix B – Software Assurance](#), which describes rules on purchasing SA and additional benefits available to SA customers.
 - [Appendix C – Professional Services](#), which lists the Professional Services offered through Microsoft Volume Licensing.
 - [Appendix D – Program Agreement Supplemental Terms](#), which provides additional terms for Microsoft Volume Licensing Program Agreements.
 - [Appendix E – Product Promotions](#), which lists Product promotions that are not otherwise on the Price List.
 - [Appendix F – Storage Array Terms](#), which provided additional terms for Storage Array devices.
- [Index](#), which lists all the Products referenced in the Product Terms and identifies where they are located.

How to Navigate a Product Entry

Each Software Product Entry includes four sections: Program Availability, Product Conditions, Use Rights, and Software Assurance. Each Online Services Product Entry includes two sections: Program Availability and Product Conditions.

1. Program Availability identifies, for each Product, the offering type, point count (where applicable), and availability across volume licensing programs.

1. Program Availability										
Products	DA	L	L/SA	SA	OL	S/S+	MPSA	UV/OVS	EA/EAS	UVS-ES
Windows MultiPoint Server 2012 Standard	12/12	5	8	3						
Windows MultiPoint Server 2012 Premium	12/12	10	15	5						

Point values are for one year

Open License

Hovering a cursor over the column headings and cell values displays additional information

A green cell means the Product is available in the column's Program

2. Product Conditions provides additional information related to acquiring the Product, such as prerequisites for purchase, prior versions, and the applicable Product Pool.

2. Product Conditions		
Prior Version: Visual Studio 2012 (8/12)	Product Pool: Applications	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): N/A
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): All except MSDN OS	Transition Eligible: N/A	True Up Eligible: N/A
UTD Discount: N/A		

Hovering a cursor over blue text displays additional information

A gray cell means the attribute does not apply to the Product(s) listed in 1. Program Availability

2.1 License Grant for SQL Server Parallel Data Warehouse Developer
The Licensed Users under Visual Studio Professional with MSDN, Visual Studio Premium 2013 with MSDN, Visual Studio Test Professional 2013 with MSDN are deemed to have one license for SQL Server 2012 Parallel Data Warehouse Developer.

3. Use Rights identifies the License Terms for each Software Product, including the Universal License Terms, the applicable License Model, and any Product-Specific License Terms. References in Customer's volume licensing agreement to "Product Use Rights" refer to the terms included in the Use Rights section of each Software Product Entry. Terms for Online Services are in the OST.

3. Use Rights		
License Terms: Universal Servers/CAL	Product-Specific License Terms: N/A	Additional Software: All
Client Access Requirement: All	External User Access Requirement: CAL	Included Technologies: N/A
Notices: N/A		
3.1 Server Software Access		
Base Access License	Project Server 2013 CAL Project Online User SL	Pro Pro

Blue underline text is a "hyperlink" redirecting to more details

Server Software Access table identifies the licenses needed to access the Servers or manage devices using the Products listed in 1. Program Availability

4. Software Assurance identifies terms and conditions associated with SA coverage.

4. Software Assurance		
SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: All (except Developer and Parallel Data Warehouse)
License Mobility: All (except Developer and Parallel Data Warehouse)	Migration Rights: Product List – March 2014 and March 2015	Roaming Use Rights: N/A
Self Hosting: All (except Developer)		
4.1 SQL Server 2014 Enterprise Core – Unlimited Virtualization Customer may run any number of instances of the server software in any number of OSEs on any Licensed Software on all of its core licenses for the Server.		

Identifies where information on migration paths from one version of software to another version is located

Clarifications and Summary of Changes to this Document

Below are recent additions, deletions and other changes to the Product Terms. Also listed below, are clarifications of Microsoft policy in response to common customer questions.

Additions	Deletions
System Center 2016 Data Protection Manager per OSE	System Center 2016 Client Management Suite per OSE
System Center 2016 Data Protection Manager per User	System Center 2016 Client Management Suite per User
System Center 2016 Operations Manager per OSE	Microsoft Azure StorSimple Monetary Commitment-1 (8100 device)
System Center 2016 Operations Manager per User	Microsoft Azure StorSimple Monetary Commitment-1 (8600 device)
System Center 2016 Orchestrator per OSE	Operations Management Suite E1 Add-on
System Center 2016 Orchestrator per User	Operations Management Suite E2 Add-on
System Center 2016 Service Manager per OSE	Operations Management Suite E1
System Center 2016 Service Manager per User	Operations Management Suite E1 From SA
Microsoft Azure StorSimple Plan with Device (8100 device)	Operations Management Suite E2
Microsoft Azure StorSimple Plan with Device (8600 device)	Operations Management Suite E2 From SA
Microsoft Azure StorSimple Plan 8100 Renewal (no device)	Operations Management Suite: Insights and Analytics
Microsoft Azure StorSimple Plan 8600 Renewal (no device)	Operations Management Suite: Automation and Control
Operations Management and Security E1 Add-on	Operations Management Suite: Security and Compliance
Operations Management and Security E2 Add-on	Operations Management Suite: Backup and Disaster Recovery
Operations Management and Security E1	Office 365 Advanced eDiscovery
Operations Management and Security E1 From SA	Microsoft Learning MTA 250 Exam Site License
Operations Management and Security E2	Yammer Enterprise
Operations Management and Security E2 From SA	
Operations Management and Security: Insights and Analytics	
Operations Management and Security: Automation and Control	
Operations Management and Security: Security and Compliance	
Operations Management and Security: Backup and Disaster Recovery	
Office 365 Advanced Compliance	
Microsoft Learning MTA/MCA Certification 125 Exam Site License	
Microsoft Learning MOS/MCE Certification 125 Exam Site License	
Microsoft Learning MTA/MCE Certification 500 Exam Site License	

Software

Microsoft Dynamics 365 On-premises: The Migration License for Microsoft Dynamics CRM Software Assurance clause from Section 4 has been removed and a reference to the December 2016 Product Terms has been added to the Migrations Rights cell of Section 4's Attribute table to denote where this information resides.

[System Center](#): System Center 2016 Client Management Suite was the last version of Client Management Suite. Each of the four component products of Client Management Suite are now licensed as separate products.

[Visual Studio Team Foundation Server](#): The Software Assurance Migration for Customers with Visual Studio Team Foundation Server 2015 with SQL 2014 Technology and Software Assurance Migration for Customers with Visual Studio Team Foundation Server 2015 CAL clauses from Section 4 have been removed and a reference to the December 2016 Product Terms has been added to the Migrations Rights cell of Section 4's Attribute table to denote where this information resides.

Online Service Specific Terms

[Microsoft Azure Plans](#): Operations Management Suite has been renamed Operations Management and Security.

[Office 365 Services](#): Office 365 Advanced eDiscovery has been renamed Office 365 Advanced Compliance.

Appendix E

[Azure Compute Capacity Promotion](#): The Azure Compute Capacity Promotion has been extended to March 31, 2017.

[System Center Client Management Suite Promotion](#): The System Center Client Management Suite Promotion expired December 31, 2016.

[Table of Contents](#) / [Glossary](#) / [Index](#)

License Terms

All instances of the “Product Use Rights” in Customer’s volume licensing agreement refer to the terms identified in the “Use Rights” section of each Product Entry. For each Product, this includes the Universal License Terms, applicable License Model Terms and any Product-Specific License Terms in the Product Entry.

For Online Services, references to “Product Use Rights” in Customer’s volume licensing agreement refer to the OST. If a software Product includes both software and online services, the online services will be governed by the terms in the OST and all the software will be governed by these License Terms.

Universal License Terms

Universal License Terms apply to all software Products licensed through Microsoft Volume Licensing (except where specifically noted in the License Model Terms and/or the Product-Specific License Terms).

1. Definitions

Terms used in the Product Terms but not defined in the [Glossary](#) will have the definition provided in Customer’s volume licensing agreement.

2. Customer’s Use Rights

If Customer complies with its volume licensing agreement, it may use the software as expressly permitted in the Product Terms. Customer needs a [License](#) for each Product and separately licensed functionality used on a device or by a user.

3. Rights to Use Other Versions and Lower Editions

For any permitted copy or [Instance](#), Customer may create, store, install, run or access in place of the version licensed, a copy or [Instance](#) of a prior version, different permitted language version, different available platform version (for example, 32 bit or 64 bit) or a permitted lower edition. The use rights for the licensed version still apply. Licenses for prior versions and lower editions do not satisfy the licensing requirements for a Product.

4. Third Party Software

The software may contain third party proprietary programs or components that are licensed under separate terms that are presented to Customer during installation or in the “ThirdPartyNotices” file accompanying the software. The software may also contain third party open source programs that Microsoft, not the third party, licenses to Customer under Microsoft’s license terms.

5. Pre-Release Code, Updates or Supplements, Additional Functionality

Microsoft may offer updates or supplements to the Products. Customer may use the updates or supplements to the Products, pre-release code, additional functionality and optional add-on services to the Products, subject to specific terms (if any) that accompany them. Some Products require automatic updates, as described in the Product-Specific License Terms.

6. Restrictions

Customer may not (and is not licensed to) use the Products to offer commercial hosting services to third parties, work around any technical limitations in the Products or restrictions in Product documentation, or separate the software for use in more than one [OSE](#) under a single License (even if the OSEs are on the same physical hardware system), unless expressly permitted by Microsoft. Rights to access the software on any device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.

7. Software Assurance

SA coverage may grant additional use rights to Customer. These additional rights end at the expiration of the SA coverage for the [License](#), unless otherwise noted in the benefit description.

8. Outsourcing Software Management

Customer may install and use licensed copies of the software on [Servers](#) and other devices that are under the day-to-day management and control of third parties, provided all such Servers and other devices are and remain fully dedicated to Customer’s use. Customer is responsible for all of the obligations under its volume licensing agreement regardless of the physical location of the hardware upon which the software is used.

9. License Assignment and Reassignment

Before Customer uses software under a [License](#), it must assign that [License](#) to a device or user, as appropriate. Customer may reassign a [License](#) to another device or user, but not less than 90 days since the last reassignment of that same [License](#), unless the reassignment is due to (i) permanent hardware failure or loss, (ii) termination of the user’s employment or contract or (iii) temporary reallocation of [CALs](#), Client [Management Licenses](#) and user or device [SLs](#) to cover a user’s absence or the unavailability of a device that is out of service. Customer must remove the software or block access from the former device or to the former user. SA coverage and any Licenses that are granted or acquired in connection with SA coverage may be reassigned only with the underlying qualifying [License](#). Different terms apply to the reassignment of Windows desktop operating system per device licenses and SA coverage, as detailed in the [Windows Product Entry](#).

10. Technical Measures

Microsoft may use technical measures to enforce terms that restrict Customer's use of certain versions of Product and may verify compliance with those terms as provided in Customer's volume license agreement. Some Products are protected by technological measures and require activation or validation, as well as a product key, to install or access them.

10.1 Activation and validation

Successful activation or validation verifies that a software Product has been correctly installed, the product key is not stolen, and that no changes have been made to validation, licensing, or activation functions of the software. Customer's right to use the software after the time specified in the software Product may be limited unless it is activated. Customer is not licensed to continue using the software if it has unsuccessfully attempted to activate. Each device that has not activated by a Key Management Service (KMS) must use a Multiple Activation Key (MAK). Customer may not circumvent activation or validation.

10.2 Product Keys

An assigned product key is required for licensed use of the software. All product keys are Confidential Information of Microsoft. Notwithstanding anything to the contrary in Customer's volume licensing agreement, Customer may not disclose product keys to third parties. Customer may not provide unsecured access to its key management service (KMS) machines over an uncontrolled network. In the event of unauthorized use or disclosure of product keys or KMS keys, Microsoft may prevent further activations, deactivate or block product keys from activation or validation, and take other appropriate action.

11. Notices

Where indicated in the Use Rights section of each Product Entry, the following notices apply:

11.1 Internet-based Features

Software Products may contain features that connect and send information over the Internet, without additional notice to Customer, to Microsoft's systems and those of its Affiliates and service providers. Use of that information is described in the privacy statement available in each software Product.

11.2 Bing Maps

The Product may include use of Bing Maps. Any content provided through Bing Maps, including geocodes, can only be used within the product through which the content is provided. Customer's use of Bing Maps is governed by the Bing Maps End User Terms of Use available at <http://go.microsoft.com/?linkid=9710837> and the Bing Maps Privacy Statement available at <http://go.microsoft.com/fwlink/?LinkID=248686>.

11.3 H.264/AVC Visual Standard, the VC-1 Video Standard, and the MPEG-4 Part 2 Visual Standard

This software may include H.264/AVC, VC-1, and MPEG-4 Part 2 visual compression technology. MPEG LA, L.L.C. requires this notice: THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, THE MPEG-4 PART 2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE ("VIDEO STANDARDS") AND/OR (ii) DECODE AVC, VC-1, MPEG-4 PART 2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE www.mpegla.com. For clarification purposes, this notice does not limit or inhibit the use of the software for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of content with the VIDEO STANDARDS compliant technologies for distribution to third parties.

12. Font Components, Images, and Sounds

While Customer runs the software, it may access and use icons, images, sounds and media included with the software only from a [Licensed Device](#) and may use the fonts included with or installed by that software to display and print content. Customer may only embed fonts in content as permitted by the embedding restrictions in the fonts; and temporarily download them to a printer or other output device to print content.

13. Included Technologies

Products may include other Microsoft technology components subject to their own license terms, as indicated in the Use Rights section of each Product Entry. If separate terms for these components are not addressed in the Product-Specific License Terms, they may be found in a separate folder in the Product's installation directory or through the Product's unified installer.

14. Benchmark Testing

Customer must obtain Microsoft's prior written approval to disclose to a third party the results of any benchmark test of any [Server](#) Product or Microsoft Desktop Optimization Pack. This does not apply to Windows Server.

15. Multiplexing

Multiplexing or pooling to reduce direct connections with the software does not reduce the number of required [Licenses](#).

16. Administrative and Support Rights

Customer may allow access to server software running in any permitted [OSE](#) by two users without CALs solely for administrative purposes. Customer may also allow remote access to other Products solely for purposes of providing technical product support to [Licensed Users](#) or on [Licensed Devices](#).

17. Distributable Code

The software may include code that Customer is permitted to distribute in programs it develops if it complies with the terms below.

17.1 Right to Use and Distribute

The code and text files listed below are “Distributable Code.”

- REDIST.TXT Files: Customer may copy and distribute the object code form of code listed in REDIST.TXT files and in OTHER-DIST.TXT files, as well as any code marked as “Silverlight Libraries”, Silverlight “Client Libraries” and Silverlight “Server Libraries”.
- Sample Code, Templates, and Styles: Customer may modify, copy, and distribute the source and object code form of code marked as “sample”, “template”, “simple styles” and “sketch styles.”
- Third Party Distribution: Customer may permit distributors of its programs to copy and distribute the Distributable Code as part of those programs.
- Image Library: Customer may copy and distribute images, graphics and animations in the Image Library as described in the software documentation.

17.2 Distribution Requirements

If Customer distributes any Distributable Code. Customer must:

- Only distribute it with Customer’s programs, where Customer’s programs provide significant primary functionality to the Distributable Code;
- require distributors and external end users to agree to terms that protect the Distributable Code at least as much as Customer’s volume licensing agreement, including the Product Terms;
- indemnify, defend, and hold harmless Microsoft from any claims, including attorneys’ fees, related to the distribution or use of Customer’s programs, except to the extent that any claim is based solely on the Distributable Code included in Customer’s programs.

17.3 Distribution Limitations

Customer may not:

- alter any copyright, trademark or patent notice in the Distributable Code;
- use Microsoft’s trademarks in Customer’s programs’ names or in a way that suggests its programs come from or are endorsed by Microsoft;
- distribute Distributable Code in or with any malicious or, deceptive programs or in an unlawful manner; or
- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that the code be disclosed or distributed in source code form, or that others have the right to modify it.

18. Software Plus Services

Microsoft may provide services with Products through software features that connect with Microsoft or service provider computer systems over the Internet. It may change or cancel the services at any time. Customer may not use the services in any way that could harm them or impair anyone else’s use of them. Customer may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

[Table of Contents](#) / [Glossary](#) / [Index](#)

License Model Terms

The License Model for each Product is identified in the Use Rights section of the Product Entry. License Model terms apply to all software Products licensed under that License Model, as specified in the Product Entry and subject to any exceptions and other terms noted in the Product-Specific License Terms.

Desktop Applications

Device License

1. Customer may install any number of copies of the software on a [Licensed Device](#) and on any [Server](#) dedicated to Customer’s use for each [License](#) it acquires.
2. Unless Customer licenses the software as an Enterprise Product or on a company-wide basis, it may also install the software on a single portable device for use by the [Primary User](#) of the [Licensed Device](#).
3. Any number of users may use the software running on a [Licensed Device](#), but only one user may access and use the software at a time.
4. Remote use of the software running on a [Licensed Device](#) is permitted for the [Primary User](#) from any device or for any other user from another [Licensed Device](#).

- Remote use of the software running on a [Server](#) dedicated to Customer's use is permitted for any user from a [Licensed Device](#).

Media Elements and Templates

Microsoft grants Customer a license to copy, distribute, perform and display media elements (images, clip art, animations, sounds, music, video clips, templates and other forms of content) included with the software and the Office web apps in projects and documents, except that Customer may not sell, license or distribute copies of any media elements by themselves or as a product if the primary value of the product is the media elements.

Desktop Operating Systems

Device License

- Customer may install one copy of the software on a [Licensed Device](#) or within a local virtual hardware system on a [Licensed Device](#) for each [License](#) it acquires.
- Customer may use the software on up to two processors.
- Local use is permitted for any user.
- Remote use is permitted for the [Primary User](#) of the [Licensed Device](#) and for any other user from another [Licensed Device](#) or a Windows VDA [Licensed Device](#).
- Only one user may access and use the software at a time.
- Customer may connect up to 20 devices to the [Licensed Device](#) for file sharing, printing, Internet Information Services, Internet Connection Sharing or telephony services.
- An unlimited number of connections are allowed for KMS activation or similar technology.

Adobe Flash Player

The software may include a version of Adobe Flash Player. Customer agrees that its use of the Adobe Flash Player is governed by the license terms for Adobe Systems Incorporated at <http://go.microsoft.com/fwlink/?linkid=248532>. Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Per Core/CAL

Server Licenses (per core)

- Customer may use the server software on a [Licensed Server](#), provided it acquires sufficient [Server](#) licenses as described below.
- The number of [Licenses](#) required equals the number of [Physical Cores](#) on the [Licensed Server](#), subject to a minimum of 8 [Licenses](#) per [Physical Processor](#) and a minimum of 16 [Licenses](#) per [Server](#).
- Datacenter edition permits use of the server software in any number of [OSEs](#) on the [Licensed Server](#).
- Standard edition:
 - Standard edition permits use of the server software in two [OSEs](#) on the [Licensed Server](#).
 - Standard edition permits use of one [Running Instance](#) of the server software in the [Physical OSE](#) on the [Licensed Server](#) (in addition to two [Virtual OSEs](#)), if the [Physical OSE](#) is used solely to host and manage the [Virtual OSEs](#).
 - Customer may assign additional Standard edition [Licenses](#) to the [Licensed Server](#) equal to the number specified in 2 above and use the server software in two additional [OSEs](#) on the [Licensed Server](#).
- As long as the total numbers of [Licenses](#) and [Physical Cores](#) remains the same, [License](#) reassignment is permitted any time Customer repartitions a single piece of hardware.
- As a one-time alternative to assigning base [CALs](#) per user or per device, a number of base [CALs](#) may be dedicated to an [Instance](#) of the server software on a single [Server](#) (per server mode) to permit up to the same number of users or devices to concurrently access that [Instance](#).

Access Licenses

- Except as described here and noted in the [Product-Specific License Terms](#), all server software access requires [CALs](#) or [CAL Equivalent Licenses](#).
- [CALs](#) are not required for access by another [Licensed Server](#).
- [CALs](#) are not required to access server software running a [Web Workload](#) or [HPC Workload](#).
- [CALs](#) are not required for access in a [Physical OSE](#) used solely for hosting and managing [Virtual OSEs](#).

Server/CAL

Server Licenses (per Instance)

Customer may use one [Running Instance](#) of server software in either a [Physical OSE](#) or [Virtual OSE](#) on a [Licensed Server](#) for each [License](#) it acquires.

Access Licenses

- Except as described here and noted in the [Product-Specific License Terms](#), all server software access requires [CALs](#) or [CAL Equivalent Licenses](#).
- [CALs](#) are not required for access by another [Licensed Server](#).

Per Core

For Products under the Per Core License Model, Customer must choose either Licensing by [Physical Core](#) on a [Server](#) or Licensing by Individual [Virtual OSE](#). The terms for each are set forth below.

Server Licenses (per core) – Licensing by Physical Core on a Server

1. Customer may use the server software on a [Licensed Server](#), provided it acquires sufficient [Server](#) Licenses as described below.
2. The number of [Licenses](#) required equals the number of [Physical Cores](#) on the [Licensed Server](#) subject to a minimum of four [Licenses](#) per [Physical Processor](#).
3. For Enterprise edition, Customer may use any number of [Running Instances](#) of the server software on the [Licensed Server](#) in a number of [Physical OSEs](#) and/or [Virtual OSEs](#) equal to the number of licenses assigned to it.
4. For each additional Enterprise edition [License](#) that Customer assigns beyond the number of [Licenses](#) required under paragraph 2 above, it may use of the server software in one additional [OSE](#) on the [Licensed Server](#).
5. For other editions, Customer may use any number of [Running Instances](#) of the server software only in the [Physical OSE](#) on the [Licensed Server](#).

Server Licenses (per core) – Licensing by Individual Virtual OSE

1. Customer may use any number of [Running Instances](#) of the server software in any [Virtual OSE](#) on the [Licensed Server](#), provided it acquires sufficient [Licenses](#) as described below.
2. The number of [Licenses](#) required equals the number of [Virtual Cores](#) in the [Virtual OSE](#), subject to a minimum of four [Licenses](#) per [Virtual OSE](#).
3. If any [Virtual Core](#) is at any time mapped to more than one [Hardware Thread](#), Customer needs a License for each [Hardware Thread](#) to which it is mapped.

Management Servers

Management Licenses

The Management License version, not the version of software used, determines the version of applicable License Terms (including use under downgrade rights notwithstanding terms to the contrary).

Server Management Licenses (per core)

1. Customer may use the software on any [Server](#) dedicated to its use to [Manage OSEs](#) on a [Licensed Server](#), provided it acquires sufficient [Server](#) Licenses as described below.
2. The number of [Licenses](#) required equals the number of [Physical Cores](#) on the [Licensed Server](#), subject to a minimum of 8 [Licenses](#) per [Physical Processor](#) and a minimum of 16 [Licenses](#) per [Server](#).
3. Datacenter edition permits use of the server software to Manage any number of [OSEs](#) on the [Licensed Server](#).
4. Standard edition:
 - Standard edition permits use of the software to Manage up to two [OSEs](#) on the [Licensed Server](#).
 - Standard edition permits Management of the [Physical OSE](#) on the [Licensed Server](#) (in addition to two [Virtual OSEs](#)), if the [Physical OSE](#) is used solely to host and Manage [Virtual OSEs](#).
 - Customer may assign additional Standard edition [Licenses](#) to the [Licensed Server](#) equal to the number specified in 2 above and Manage two additional [OSEs](#).
5. [OSEs](#) running [Server](#) operating systems require Server [Management Licenses](#).

Client Management Licenses (per OSE or user)

1. Customer may use the software to Manage an [OSE](#) on a [Licensed Device](#) or [OSEs](#) on devices used by a [Licensed User](#) for each Client Management License it acquires.
2. [OSEs](#) running operating systems other than [Server](#) operating systems require Client Management Licenses or [Management License Equivalent Licenses](#).
3. The number of Client Management Licenses required depends on [License](#) type (per [OSE](#) or user) assigned.
4. Management of an [OSE](#) accessed by more than one user requires an [OSE](#) Client Management License or a User Client Management License for each user.

Management Licenses are not required for:

1. [OSEs](#) in which there are no [Running Instances](#) of software;
2. Any of Customer's network infrastructure devices functioning solely for the purpose of transmitting network data and not running Windows Server software;
3. Conversion of [OSEs](#) from Physical to Virtual; or
4. Any device solely monitored or managed for the status of its hardware components with respect to system temperature, fan speed, power on/off, system reset or CPU availability.

Data Sets

Customer may not copy or distribute any data set (or any portion of a data set) included in the software.

Specialty Servers

Server Licenses (per Instance)

Customer may use one [Running Instance](#) of server software in either a [Physical OSE](#) or [Virtual OSE](#) on a [Licensed Server](#) for each [Server](#) License it acquires

Developer Tools

User Licenses

1. One [Licensed User](#) may use any number of copies of the software and any prior version on any device dedicated to Customer's use for each User License it acquires.
2. [Licensed Users](#) may use the software for evaluation and to develop, test, and demonstrate Customer's programs. These rights include the use of the software to simulate an end user environment to diagnose issues related to its programs.
3. The software is not licensed for use in a [Production Environment](#).

Additional License Terms for MSDN Subscriptions

In addition to the rights in the License Model Terms, Customer may allocate an MSDN subscription for each [License](#) it acquires. For MSDN subscriptions, the "Software" means software made available to Customer's subscription level via MSDN Subscriber Downloads. Any online service made available with Customer's MSDN subscription may not be used in a [Production Environment](#).

Running the Software on Microsoft Azure Platform Services

1. The [Licensed User](#) may run the Software on Microsoft Azure Platform Services during the term of its MSDN subscription.
2. The use of the Software remains subject to the terms and conditions of Customer's volume licensing agreement and any terms that come with the Software.
3. The Developer Tools License Model Terms apply to the use of the Software and Azure MSDN Dev/Test offers, except that the [Licensed User](#) may not run Office Professional Plus or System Center Virtual Machine Manager for production use on Microsoft Azure Platform Services.

Additional Requirements

To run Software on Microsoft Azure Platform Services Customer must activate its MSDN subscription by linking its Microsoft account to the MSDN subscription.

Acceptance Testing and Feedback

Customer's end users may access the Software, and online services made available with Customer's MSDN subscription, to perform acceptance tests or to provide feedback on its programs.

Windows Server 2016 Remote Desktop Services

Up to 200 anonymous users at a time may use the Remote Desktop Services feature of the Windows Server software to access online demonstrations of Customer's programs.

Windows Embedded Product

Each Windows Embedded Product is licensed under the terms that come with it, including any Microsoft obligations related to defense of infringement and misappropriation claims. These terms replace the corresponding terms in Customer's volume licensing agreement. Each [Licensed User](#) may install and use an unlimited number of copies of the licensed Windows Embedded Product.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Software

Advanced Threat Analytics

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Advanced Threat Analytics 2016 Client Management License per OSE	8/15		2	1				P	A	A	A,ST
Advanced Threat Analytics 2016 Client Management License per User	8/15		2	1				P	A	A	

2. Product Conditions

Prior Version: N/A	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

2.1 Country Restrictions

Customer may not download Advanced Threat Analytics 2016 for use or distribution in the People's Republic of China.

3. Use Rights

License Terms: Universal; Management Servers	Product-Specific License Terms: Yes	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: Windows Software Components
Notices: Internet-based Features		

3.1 Management License

Client Management License	Advanced Threat Analytics 2016 (User or OSE ML)	Management License Equivalent License (refer to Appendix A)

3.2 Usage Requiring a Management License

[Licenses](#) are only required for client [OSEs](#) (or server [OSEs](#) used as client [OSEs](#)) that are on or accessed by end user devices authenticated by an Active Directory managed by Advanced Threat Analytics.

3.3 GNU Lesser General Public Licensed libraries

[Licensed User](#) may reverse engineer, decompile or disassemble the Advanced Threat Analytics software, or otherwise attempt to derive the source code for the Advanced Threat Analytics Server software solely to the extent required to debug changes to any libraries licensed under the GNU Lesser General Public License that may be included with and linked to by the software.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: Yes	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: N/A	Roaming Rights: N/A
Self Hosting: Yes	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

BizTalk

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
BizTalk Server 2016 Branch Edition	12/16	25	38	13	OM			OM, P	A,SP	A	A
BizTalk Server 2016 Branch IDC	12/16										
BizTalk Server 2016 Enterprise Edition	12/16	200	300	100	OM			OM, P	A,SP	A	A
BizTalk Server 2016 Standard Edition	12/16	50	75	25	OM			OM, P	A,SP	A	A

Attachment E - Page 64 of 245

[Table of Contents](#)

[Introduction](#)

[License Terms](#)

[Software](#)

[Online Services](#)

[Glossary](#)

[Appendices](#)

[Index](#)

BizTalk Server 2016 Standard Edition IDC

12/16

2. Product Conditions

Prior Version: BizTalk Server 2013 R2 (6/14)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: All	Reduction Eligible: N/A
Reduction Eligible (SCE): All (except Branch IDC)	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Per Core	Product-Specific License Terms: Branch and Standard	Additional Software: All editions
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: Windows Software Components and Office web apps
Notices: Internet-based Features		

3.1 BizTalk Server Branch and Standard Edition

Customer may not use the server software on a [Server](#) that is part of a networked cluster or in an [OSE](#) that is part of a networked cluster of [OSEs](#) on the same [Server](#).

3.2 BizTalk Server Branch Edition

Customer may [Run Instances](#) of the software on [Licensed Servers](#) only at the endpoint of its internal network (or edge of its organization) to connect business events or transactions with activities processed at that endpoint; provided, the [Licensed Server](#) may not:

- act as the central node in a “hub and spoke” networking model,
- centralize enterprise-wide communications with other Servers or devices; or
- automate business processes across divisions, business units, or branch offices.

3.3 Additional Software

Administration and Monitoring Tools	ADOMD.NET	BizTalk Server Related Schemas and Templates
Business Activity Monitoring (“BAM”) Client	BAM Alert Provider for SQL Notification Services	BAM Event APIs and Interceptors and Administration Tools
Business Activity Services	Business Rules Component	Development Tools
HTTP Receive Adapter	Master Secret Server/Enterprise Single Sign-On	MQHelper.dll
MQSeries Agent	MSXML	SOAP Receive Adapter
Software Development Kit(s)	SQLXML	UDDI
Windows Communication Foundation Adapters	Windows SharePoint Services Adapter Web Services	

4. Software Assurance

SA Benefits: Server	Disaster Recovery: All editions	Fail-Over Rights: N/A
License Mobility: All editions	Migration Rights: Product List - December 2014	Roaming Rights: N/A
Self Hosting: All editions (except Branch)	SA Equivalent Rights: N/A	

4.1 Biz Talk Server 2013 R2 Enterprise – Unlimited Virtualization

Customer may run any number of [Instances](#) of the server software in any number of [OSEs](#) on any [Licensed Server](#) for which it has full SA coverage on all of its [Server](#) (per core) [Licenses](#).

[Table of Contents](#) / [Glossary](#) / [Index](#)

CAL Suites

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Core CAL Suite (Device and User)		(1)	2	1				E, P	E	ED	ED,SD,ST
Core CAL Suite Bridge for Office 365 (User SL)								P	E		
Core CAL Suite Bridge for Office 365 and Microsoft Intune (User SL)									E		
Core CAL Suite Bridge for Microsoft Intune (User SL)									E		

Attachment E - Page 65 of 245

[Table of Contents](#)
[Introduction](#)
[License Terms](#)
[Software](#)
[Online Services](#)
[Glossary](#)
[Appendices](#)
[Index](#)

Core CAL Suite Bridge for Enterprise Mobility+ Security (User SL)				P	E		
Enterprise CAL Suite (Device and User)	(2)	8	2	E, P	EP	ED	ED,SD,ST
Enterprise CAL Suite Bridge for Office 365 (User SL)				P	E		
Enterprise CAL Suite Bridge for Office 365 From SA (User SL)					E		
Enterprise CAL Suite Bridge for Office 365 and Microsoft Intune (User SL)					E		
Enterprise CAL Suite Bridge for Microsoft Intune (User SL)					E		
Enterprise CAL Bridge for Enterprise Mobility + Security (User SL)				P	E		
Enterprise CAL Bridge for Enterprise Mobility + Security From SA (User SL)					E		

2. Product Conditions

Prior Version: N/A	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: Core CAL or Enterprise CAL Suite		

2.1 Process to Determine Applicable Use Rights for CAL Suites

A CAL Suite License is version-less and the access rights are determined by the status of the SA coverage on it. If SA coverage lapses, access rights under perpetual Licenses are determined based on the use rights in effect for the versions that were current prior to the lapse.

2.2 Components of CAL Suite

Refer to [Appendix A](#), CAL/Management License Equivalent Licenses chart for the current components of the Core CAL Suite and the Enterprise CAL Suite.

2.3 Online Services Included with Enterprise CAL Suite

Enterprise CAL Suite with active SA coverage also includes the rights to Exchange Online Archiving for Exchange Server, Data Loss Prevention, and Exchange Online Protection. For customers under Microsoft Business Agreements dated prior to October 2010 and Enrollments dated prior to July 2011, purchase and use of the Online Services included with Enterprise CAL Suite is governed by the Supplemental Terms for Online Services used with Software – Legacy Agreements in Appendix A – Program Agreement Supplemental Terms in the June 2015 Product List at <http://go.microsoft.com/?linkid=9839207>.

2.4 CAL Suite Bridge for O365, for O365 & Intune, and for Intune

2.4.1 CAL Suite Bridges Requirements

A CAL Suite Bridge may be required when replacing a CAL Suite with a comparable software and Online Service combination. When a CAL Suite Bridge is required the number of CAL Suite Bridge User SLs should be the same number of User SLs for the qualifying Online Service.

A CAL Suite Bridge is an Enterprise Product, and may only be licensed in conjunction with its qualifying Online Service to satisfy the Organization Wide requirement of either that CAL Suite Bridge or its parent CAL Suite.

CAL Suite Bridge	Parent CAL Suite	Qualifying Online Services
Core CAL Suite Bridge for Office 365*	Core CAL Suite	Office 365 Enterprise E1, or Office 365 Enterprise E3, or Office 365 Enterprise E5
Core CAL Suite Bridge for Office 365 and Microsoft Intune	Core CAL Suite	Office 365 Enterprise E1 and Microsoft Intune, or Office 365 Enterprise E3 and Microsoft Intune, or Office 365 Enterprise E5 and Microsoft Intune
Core CAL Suite Bridge for Microsoft Intune	Core CAL Suite	Microsoft Intune
Core CAL Suite Bridge for Enterprise Mobility + Security*	Core CAL Suite	Enterprise Mobility + Security E3, or Enterprise Mobility + Security E5
Enterprise CAL Suite Bridge for Office 365*	Enterprise CAL Suite	Office 365 Enterprise E3, or Office 365 Enterprise E5
Enterprise CAL Suite Bridge for Office 365 and Microsoft Intune	Enterprise CAL Suite	Office 365 Enterprise E3 and Microsoft Intune, or Office 365 Enterprise E5 and Microsoft Intune
Enterprise CAL Suite Bridge for Microsoft Intune	Enterprise CAL Suite	Microsoft Intune
Enterprise CAL Suite Bridge for Enterprise Mobility + Security*	Enterprise CAL Suite	Enterprise Mobility + Security E3, or Enterprise Mobility + Security E5

*CAL Suite Bridge From SA User SLs require fully paid, perpetual Licenses with active SA for the equivalent Parent CAL Suite. CAL Suite Bridge From SA User SL may also be purchased instead of Subscription Licenses for the Products if the Subscription License was purchased at least three years prior to the purchase of the From SA User SL.

2.4.2 Student Only CALs (Academic Open License and Academic Select)

Student Only CALs are restricted to license student owned PCs or institution owned PCs dedicated to an individual student and are not for use in labs or classrooms.

3. Use Rights

License Terms: Universal ; Server/CAL , Per Core/CAL , Management Server	Product-Specific License Terms: N/A	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: N/A
Notices: N/A		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - March 2014 (Forefront United Access Gateway 2010)	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

4.1 Extended Use Rights for Secure Productive Enterprise Customers

For qualifying customers, the Secure Productive Enterprise or a combination of Office 365 and Enterprise Mobility + Security provides access rights to the component service of Exchange Online Archiving for Exchange Server. “Qualifying Customers” are Enterprise Enrollment or Enterprise Subscription Enrollment customers who have active Software Assurance coverage for the Enterprise CAL Suite as of November 30, 2014.

Qualifying Customers licensed for Secure Productive Enterprise or the combination of Office 365 and Enterprise Mobility + Security have the same access to Exchange Online Archiving for Exchange Server as Enterprise CAL Suite provided.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Core Infrastructure Server (CIS) Suite

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Core Infrastructure Server Suite Standard		1	3	2	OM			OM, P	A, SP	A	A
Core Infrastructure Server Suite Datacenter		15	23	8	OM			OM, P	A, SP	A	A

2. Product Conditions

Prior Version: N/A	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): All	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

2.1 Software Included with CIS Suite Standard

CIS Suite Standard includes the latest versions of Windows Server Standard and System Center Standard made available during Customer’s SA coverage.

2.2 Software Included with CIS Suite Datacenter

CIS Suite Datacenter includes the latest versions of Windows Server Datacenter and System Center Datacenter made available during Customer’s SA coverage.

3. Use Rights

License Terms: Universal	Product-Specific License Terms: All editions	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: N/A
Notices: N/A		

3.1 Applicable Use Rights

Customer’s use of CIS Suite software is governed by the applicable License Terms for the individual Products comprising the CIS Suite software as modified by these License Terms. For each [Server](#) on which Customer runs CIS Suite software, the number of [Licenses](#) required equals the number

Attachment E - Page 67 of 245

of [Physical Cores](#) on the [Licensed Server](#), subject to a minimum of 8 [Licenses](#) per [Physical Processor](#) and a minimum of 16 [Licenses](#) per [Server](#). Customer may assign additional CIS Suite Standard edition [Licenses](#) to the [Licensed Server](#) equal to the number specified in the prior sentence and run the server software in two additional [OSEs](#) and Manage two additional [OSEs](#) on the [Licensed Server](#).

3.2 Server License and Management License Assignment

For purposes of applying License Terms for Windows Server and System Center to Customer's use of CIS Suite, Customer is deemed to have assigned to the [Licensed Server](#) Windows Server and System Center Licenses equal to the number of CIS Suite [Licenses](#) assigned to the [Server](#).

3.3 Additional Terms

Customer may run a prior version or a down edition of any of the individual Products included in the CIS Suite as permitted in the license terms for that Product in the Product Terms.

All other requirements to acquire and assign [External Connector Licenses](#), [CALs](#) and [Management Licenses](#) to users or devices for access and management, as set forth in the Product Terms, remain in full force and effect.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: All editions	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - March 2014 , Product Terms - October 2016	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: Yes	

4.1 Microsoft Azure Hybrid Use Benefit

Refer to [Section 7. Microsoft Azure Hybrid Use Benefit](#) of the Microsoft Azure Product Entry for deploying Windows Server images on Microsoft Azure.

4.2 Nano Server

Customers with active SA on CIS Suite Standard or Datacenter [Licenses](#) may install, use, and Manage the Nano Server deployment option.

4.3 System Center Configuration Manager Current Branch Rights

Customers with active SA on CIS Suite Standard or Datacenter [Licenses](#) may install and use the Current Branch option of System Center Configuration Manager.

4.4 Software Assurance Rights and Benefits for Subscription Licenses

Any Subscription License Customer acquires under SCE is granted the same SA rights and benefits during the term of the subscription as [Licenses](#) with SA coverage.

4.5 Server and Cloud Enrollment (SCE) - Right to manage OSEs on Microsoft Azure under CIS Suite Licenses

SCE Customers who have met the enrollment coverage requirements and are licensed for and using CIS Suite to manage [OSEs](#) in their own data centers, may also use System Center software licensed under CIS Suite to manage their qualifying [Virtual OSEs](#) running within Microsoft Azure. For every 16 CIS Suite core [Licenses](#) or each CIS Suite processor [License](#) covered by a customer's SCE, the customer may manage up to 10 qualifying [Virtual OSEs](#) running within Microsoft Azure. Qualifying [Virtual OSEs](#) include:

- Windows Server Virtual Machine Instances (including Instances deployed under Azure HUB)
- Cloud Services instances (Web role and Worker role)
- Storage Accounts
- SQL Databases
- Websites instances

4.6 Software Assurance Renewal Offer for Windows Server and System Center

Customers who have [Licenses](#) with active SA for both of the Products in Column A of the table below may, upon expiration of that coverage, acquire SA for the corresponding CIS Suite in Column B without acquiring the underlying CIS Suite [License](#).

Column A	Column B
Windows Server Standard (2-pack Core License) System Center Standard (2-pack Core License)	Core Infrastructure Server Suite Standard (2-pack Core License)
Windows Server Datacenter (2-pack Core License) System Center Datacenter (2-pack Core License)	Core Infrastructure Server Suite Datacenter (2-pack Core License)

Customers who license and use CIS Suite (Standard or Datacenter) under this offer may no longer use software under their qualifying [Licenses](#) shown in Column A. [Licenses](#) and SA acquired under a subscription agreement do not qualify for this offer.

[Table of Contents](#) / [Glossary](#) / [Index](#)

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Forefront Identity Manager 2010 R2 - Windows Live Edition	5/12	25	38	13						A	A

2. Product Conditions

Prior Version: Forefront Identity Manager 2010 - Windows Live Edition (4/10)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

2.1 Forefront Identity Manager 2010 – Windows Live Edition

Forefront Identity Manager 2010 – Windows Live Edition is the next version for Identity Lifecycle Manager 2007 – Windows Live Edition.

3. Use Rights

License Terms: Universal ; Specialty Server	Product-Specific License Terms: All editions	Additional Software: Yes
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: N/A
Notices: N/A		

3.1 Importing identity data: Forefront Identity Manager 2010 R2 Windows Live Edition

Customer may use the software to import identity data, and changes to those data, from one or more connected data sources and to facilitate the synchronization and transfer of those data, between Customer's connected data sources and the Microsoft Passport Network / Windows Live ID service. Customer may not use the software for any other purpose.

3.2 Additional Software

Client Software		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: N/A	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Dynamics

Microsoft Dynamics 365 On-premises

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Dynamics 365 for Team Members On-premises CAL (Device and User)	12/16	(1)	2	1	OM			OM, P	A	A	A,ST
Microsoft Dynamics 365 for Customer Service On-premises CAL (Device and User)	12/16	(1)	2	1	OM			OM, P	A	A	A,ST
Microsoft Dynamics 365 for Sales On-premises CAL (Device and User)	12/16	(1)	2	1	OM			OM, P	A	A	A,ST

2. Product Conditions

Prior Version: Microsoft Dynamics CRM 2016 (12/15), Microsoft Dynamics CRM 2015 (12/14)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: All	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Server/CAL	Product-Specific License Terms: All editions	Additional Software: All editions
Client Access Requirements: All editions	External User Access Requirements: Licensed with CALs, except for (i) Customer's or its Affiliates' contractors or agents; or (ii) access through Microsoft Dynamics 365 Clients	Included Technologies: N/A
Notices: Internet-based Features , Bing Maps		

3.1 Microsoft Dynamics 365 for Team Members On-premises CAL Server Software Access

Access to server software for Team Members use.

Access License	Microsoft Dynamics 365 for Team Members On-premises CAL (Device and User)	Microsoft Dynamics 365 for Team Members, Enterprise edition (User SL)

3.2 Microsoft Dynamics 365 for Sales On-premises CAL Server Software Access

Access to server software for Sales use.

Access License	Microsoft Dynamics 365 for Sales On-premises CAL (Device and User) CAL Equivalent License (see Appendix A)	Microsoft Dynamics 365 for Sales, Enterprise edition (User SL)

3.3 Microsoft Dynamics 365 for Customer Service On-premises CAL Server Software Access

Access to server software for Customer Service use.

Access License	Microsoft Dynamics 365 for Customer Service On-premises CAL (Device and User) CAL Equivalent License (see Appendix A)	Microsoft Dynamics 365 for Customer Service, Enterprise edition (User SL)

3.4 Server Use Rights for Dynamics 365 CALs

Customers with Microsoft Dynamics 365 CALs may install and use any number of copies of the Microsoft Dynamics 365 Server software on a server.

3.5 Eligibility for Qualified Offers

Customers renewing an agreement with Microsoft Dynamics CRM CAL Licenses as of November 1, 2016 may acquire Microsoft Dynamics 365 On-premises CAL Qualified Offer Licenses in agreement renewals before October 31, 2019.

3.4 Additional Software

MarketingPilot Connector for Microsoft Dynamics CRM (Workgroup Server 2016 only)	Microsoft Dynamics CRM 2016 Best Practices Analyzer	Microsoft Dynamics CRM 2016 Microsoft Office Outlook
Microsoft Dynamics CRM 2016 Multilingual User Interface (MUI)	Microsoft Dynamics CRM 2016 Report Authoring Extensions	Microsoft Dynamics CRM Reporting Extensions for Microsoft Dynamics CRM 2016
Microsoft Dynamics CRM for supported devices	Microsoft E-Mail Router and Rule Deployment Wizard for Microsoft Dynamics CRM 2016	Microsoft Dynamics Marketing Connector for Microsoft Dynamics CRM (not Workgroup Server)
Microsoft SharePoint Grid for Microsoft Dynamics CRM 2016		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - November 2014 and June 2015 ; Product Terms December 2016	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

4.1 Server Downgrade Rights

Customer may use Microsoft Dynamics CRM Server 2016 or any previous versions of the server software in place of Microsoft Dynamics 365 Server.

4.2 Unified Service Desk (USD)

For each Microsoft Dynamics 365 for Sales On-premises CAL or Dynamics 365 for Customer Service On-premises CAL for which Customer has SA, Customer may install and use USD on a [Licensed Device](#). The right to use USD is limited to the user or device to whom the qualifying CAL is assigned.

4.3 Microsoft Dynamics CustomerSource

Microsoft Dynamics 365 On-premises CAL customers with active SA will have access to CustomerSource.

Microsoft Dynamics AX

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Dynamics AX 2012 R3 Server	5/14	(50)							A		A
Microsoft Dynamics AX 2012 R3 Store Server	5/14	(10)							A		A
Microsoft Dynamics AX 2012 R3 Standard Commerce Server Core (2-pack Core License)	5/14	(125)							A		A
Microsoft Dynamics AX 2012 R3 Self Serve CAL (Device and User)	5/14	(1)							A		A
Microsoft Dynamics AX 2012 R3 Task CAL (Device and User)	5/14	(1)							A		A
Microsoft Dynamics AX 2012 R3 Task Additive CAL (Device and User)	5/14	(1)							A		A
Microsoft Dynamics AX 2012 R3 Functional CAL (Device and User)	5/14	(15)							A		A
Microsoft Dynamics AX 2012 R3 Functional Additive CAL (Device and User)	5/14	(10)							A		A
Microsoft Dynamics AX 2012 R3 Enterprise CAL (Device and User)	5/14	(50)							A		A
Microsoft Dynamics AX 2012 R3 Enterprise Additive CAL (Device and User)	5/14	(25)							A		A

2. Product Conditions

Prior Version: Microsoft Dynamics AX 2012 R2 (12/12)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Server/CAL - Server and Store Server, Per Core - Standard Commerce Server Core	Product-Specific License Terms: All editions	Additional Software: All editions
Client Access Requirements: All editions (except Standard Commerce Server Core)	External User Access Requirements: Licensed with Server	Included Technologies: N/A
Notices: N/A		

3.1 Server Software Access

Record time resulting solely for payroll processing; record expenses solely for reimbursement; manage personal information; create requisitions and manage budgets related to these activities

Access License	Microsoft Dynamics AX 2012 R3 Self-Serve CAL	Microsoft Dynamics 365 for Team Members, Enterprise edition (User SL)

3.1.1 Additional Functionality Associated with Microsoft Dynamics AX 2012 R3 Task CAL

Record and approve any type of time and expenses; approve invoices; approve all self-serve related transactions; operate a point of sale device or a warehouse device; and operate a store manager device

Additive Access License	Microsoft Dynamics AX 2012 R3 Task CAL Microsoft Dynamics 365 for Operations, Enterprise edition (User SL) CAL Equivalent License (See Appendix A)	Microsoft Dynamics AX 2012 R3 Task Additive CAL Microsoft Dynamics 365 for Team Members, Enterprise edition (User SL)

3.1.2 Additional Functionality Associated with Microsoft Dynamics AX 2012 R3 Functional CAL

Use established operational cycles and business processes provided by the software; create and update (i) position requisitions or (ii) master data records pertaining to applicants, employees, customers, vendors, or parts catalogs; and approve all task and self-serve related transactions.

Additive Access License	Microsoft Dynamics AX 2012 R3 Functional CAL Microsoft Dynamics 365 for Operations, Enterprise edition (User SL)	Microsoft Dynamics AX 2012 R3 Functional Additive CAL CAL Equivalent License (See Appendix A)

3.1.3 Additional Functionality Associated with Microsoft Dynamics AX 2012 R3 Enterprise CAL

Unrestricted access to all the functionality in the server software across the ERP solution

Additive Access License	Microsoft Dynamics AX 2012 R3 Enterprise CAL	Microsoft Dynamics AX 2012 R3 Enterprise Additive CAL
	Microsoft Dynamics 365 for Operations, Enterprise edition (User SL)	CAL Equivalent License (See Appendix A)

3.2 Modification Right

The software may include plug-ins, runtime, and other components identified in printed or online documentation that allow Customer to extend its functionality. Customer may modify or create derivative works of these components and use those derivative works, but only with the software and only for Customer's internal purposes.

3.3 Dynamics AX Standard Commerce Server Core -- Core Factor

The [License](#) minimum per Physical Processor does not apply to Dynamics AX Standard Commerce Server Core. The number of Licenses required equals the number of [Physical Cores](#) on the [Licensed Server](#) multiplied by the applicable Core Factor located at <http://go.microsoft.com/fwlink/?LinkID=229882>.

3.4 Additional Software

Management Reporter Designer Client Software for Microsoft Dynamics AX 2012 R3 Server	Microsoft Dynamics AX 2012 R3 Windows Rich Client Software	

4. Software Assurance

SA Benefits : Server	Disaster Recovery : All editions	Fail-Over Rights : All editions (server and core licenses only)
License Mobility : All editions (server and core licenses only)	Migration Rights : Product List - June 2015	Roaming Rights: N/A
Self Hosting : All editions	SA Equivalent Rights: N/A	

4.1 Localization and Updates

Customer is eligible to receive and use updates related to government tax and regulatory requirements on [Licensed Servers](#) provided it has active SA for the [Licensed Servers](#) and [CALs](#).

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Identity Manager

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Identity Manager 2016 CAL (User)	8/15	1	2	1				P	A	A	AO,ST
Microsoft Identity Manager 2016 External Connector	8/15	125	188	63	OM			P	A	A	A

2. Product Conditions

Prior Version : Forefront Identity Manager 2010 R2 (5/12)	Product Pool : Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA) : Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms : Universal	Product-Specific License Terms : All editions	Additional Software : Yes
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: N/A
Notices: N/A		

3.1 Additional Software

Client Software		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: Yes	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: N/A	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office Applications

Office Desktop Applications

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Access 2016	10/15	1	2	1				P			
Excel 2016	10/15	1	2	1				P			
Office Standard 2016	10/15	2	3	1				P			
Office Professional Plus 2016	10/15	2(1)	4	2				E, P	E	ED	ED,SD,ST
Office Home & Student 2013 RT Commercial Use	10/12	1	2	1							
Office Multi Language Pack 2013	10/12	1	2	1				P	A		
Outlook 2016	10/15	1	2	1				P			
PowerPoint 2016	10/15	1	2	1				P			
Project Standard 2016	10/15	2	4	2				P	A		
Project Professional 2016	10/15	4(1)	6	2				P	A	A	A,AO,ST
Publisher 2016	10/15	1	2	1				P			
Skype for Business 2016	10/15	1	2	1				P	A	A	A,AO,ST
Visio 2016 Standard	10/15	1	2	1				P	A		
Visio 2016 Professional	10/15	2(1)	3	1				P	A		
Word 2016	10/15	1	2	1				P			
Work at Home for Office Standard 2016	10/15	2							A		
Work at Home for Office Professional Plus 2016	10/15	2							A		

2. Product Conditions

Prior Version: Office 2013 and Office 2013 Applications (10/12), Lync 2013 (10/12)	Product Pool: Application	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: Work at Home	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: Office Professional Plus		

2.1 Project Professional 2016

Customers who license Project Professional 2016 are deemed to have one Project Server 2016 Device CAL for each Project Professional 2016 License. The right to access Project Server 2016 under that [CAL](#) will expire when the corresponding Project Professional 2016 License expires.

2.2 Work at Home

A Work at Home License is an optional License that can be acquired only in conjunction with a full [License](#) for Office Standard or Office Professional Plus. It permits the [Primary User](#) of the software to also install and use the software on one device outside of Customer's or its Affiliates' premises (e.g., at the user's home).

2.3 Platform Independent

Customer may run either the version licensed or a different platform version, provided that the different platform version was available when the original licensed version became available. If the components of a Product suite vary by platform version, Customer may use the components of the suite that it chooses to deploy and only those components; Customer may not mix components across platform versions. SA for a platform independent License permits Customer to use, in place of the licensed Product the most current version of either platform version of the Product that becomes available during the term of coverage.

2.4 Successor Versions

Skype for Business 2016 is the successor version to Lync 2013.

2.5 Office Online Server

Customers purchasing Office Standard 2016 or Office Professional Plus 2016 licenses before August 1, 2016 may use the editing functionality described in the Office Online section [Appendix B](#) with those licenses. This right expires on August 1, 2019.

3. Use Rights

License Terms: Universal ; Desktop Applications	Product-Specific License Terms: Office suites and Office Home & Student RT Commercial Use Rights	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: Office Web Apps Server 2013 (Office suites only)
Notices: Bing Maps (Excel and Office Professional Plus); H.264/MPEG-4 and/or VC-1 (Skype for Business), Internet-based Features		

3.1 Office Home & Student 2013 RT Commercial Use Rights

Upon assigning the [License](#) to a device that is separately licensed for Office Home & Student 2013 RT, Customer may use the Office Home & Student software for commercial use, despite anything to the contrary in the Office Home & Student 2013 RT license terms.

3.2 Office Professional Plus 2016 and Office Standard 2016 – Office Home & Student 2013 RT Commercial Use

Each [Primary User](#) of a [Licensed Device](#) running Office Professional Plus 2016 or Office Standard 2016 may use the software licensed separately under an Office Home & Student 2013 RT license for commercial use, despite anything to the contrary in the Office Home & Student 2013 RT license terms.

4. Software Assurance

SA Benefits: Application	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - June 2015 (Office Multi-Language Pack and Visio Premium 2010)	Roaming Rights: Office, Project and Visio
Self Hosting: N/A	SA Equivalent Rights: N/A	

4.1 Project Professional 2016

Customers with active SA for their Project Professional License will be deemed to have SA for their corresponding complimentary Project Server CAL. That deemed SA coverage will expire when the Project Professional coverage expires.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office for Mac

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Excel 2016 for Mac	8/15	1	2	1				P			
Lync for Mac 2011	9/10	1	2	1				P			
Office 2016 for Mac Standard	8/15	2(1)	3	1				P			
Outlook 2016 for Mac	8/15	1	2	1				P			
PowerPoint 2016 for Mac	8/15	1	2	1				P			
Word 2016 for Mac	8/15	1	2	1				P			
Work at Home for Mac 2016	8/15	2									

2. Product Conditions

Prior Version: Office for Mac 2011 and Office for Mac 2011 Applications (9/10)	Product Pool: Application	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: Work at Home	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

2.1 Successor Versions

Outlook for Mac 2011 is the successor version to Entourage for Mac 2008. Lync for Mac 2011 is the successor version to Communicator for Mac 2011.

2.2 Work at Home

A Work at Home License is an optional [License](#) that can be acquired only in conjunction with a full [License](#) for Office for Mac. It permits the [Primary User](#) of the software to also install and use the software on a device outside of Customer's or its Affiliate's premises (e.g., at the user's home).

2.3 Platform Independent

Customer may run either the version licensed or a different platform version, provided that the different platform version was available when the original licensed version became available. If the components of a Product suite vary by platform version, then Customer may use the components of the suite that it chooses to deploy and only those components; Customer may not mix components across platform versions. SA for a platform independent [License](#) permits Customer to use, in place of the licensed Product the most current version of either platform version of the Product that becomes available during the term of coverage.

3. Use Rights

License Terms: Universal; Desktop Applications	Product-Specific License Terms: Office for Mac	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: Office Web Apps Server 2013 (Office suite only)
Notices: Internet-based Features		

3.1 Office Home & Student 2013 RT Commercial Use

The [Primary User](#) of an Office 2016 for Mac Standard [Licensed Device](#) may use the software licensed separately under an Office Home & Student 2013 RT license for commercial use, despite anything to the contrary in the Office Home & Student 2013 RT license terms.

4. Software Assurance

SA Benefits: Application	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - June 2015 (Communicator for Mac 2010, Entourage for Mac 2008)	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office Servers

Exchange Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Exchange Server Enterprise 2016	10/15	50	75	25				P	A	A	A
Exchange Server Enterprise 2016 CAL (Device and User)	10/15	1	2	1				P	A	A	AO,ST
Exchange Server Standard 2016	10/15	10	15	5				P	A	A	A
Exchange Server Standard 2016 CAL (Device and User)	10/1	1	2	1				P		A	AO,ST

2. Product Conditions

Prior Version: Exchange Server 2013 (10/12)	Product Pool: Server	Down Editions: Enterprise to Standard
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal; Server/CAL	Product-Specific License Terms: N/A	Additional Software: All editions
Client Access Requirements: All editions	External User Access Requirements: Licensed with Server (access to Additional Functionality requires	Included Technologies: N/A

	both Base and Additive CALs)	
Notices: N/A		

3.1 Server Software Access

Base Access License	Exchange Server 2016 Standard CAL Exchange Online Plan 1 G User SL Exchange Online Plan 2A User SL CAL Equivalent License (refer to Appendix A)	Exchange Online Plan 1 User SL Exchange Online Plan 2 User SL Exchange Online Plan 2G User SL

3.1.1 Additional Functionality Associated with Exchange Enterprise CAL

In-Place Archive, In-Place Holds (Indefinite, Query-based, and Time-based), Advanced Mobile Policies, Information Protection and Compliance, Custom Retention Policies, Per User/Distribution List Journaling, Site Mailboxes – Compliance, Data Loss Prevention

Additive Access License	Exchange Server 2016 Enterprise CAL Exchange Online Plan 2A User SL CAL Equivalent License (refer to Appendix A)	Exchange Online Plan 2 User SL Exchange Online Plan 2G User SL

3.2 Additional Software

Exchange Management Tools		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: All Server editions	Fail-Over Rights: N/A
License Mobility: All editions (server licenses only)	Migration Rights: Product List - June 2015 (External Connector)	Roaming Rights: N/A
Self Hosting: All editions	SA Equivalent Rights: N/A	

4.1 Exchange Enterprise CAL with Services 2016 Supplemental Terms and Conditions

Exchange Server Enterprise CAL with active SA coverage includes the rights to Data Loss Prevention and Exchange Online Protection. For customers under Microsoft Business Agreements dated prior to October 2010 and Enrollments dated after July 2011, the Supplemental Terms for Online Services used with Software – Legacy Agreements section of Appendix A – Program Agreement Supplement Terms in the June 2015 Product List at <http://go.microsoft.com/?linkid=9839207> apply to purchase and use of the Online Services included with Exchange Enterprise CAL with Services 2016.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Project Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Project Server 2016	5/16	50	75	25				P	A	A	A
Project Server 2016 CAL (Device and User)	5/16	1	2	1				P	A	A	A

2. Product Conditions

Prior Version: Project 2013 (10/12)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Server/CAL	Product-Specific License Terms: N/A	Additional Software: Yes
Client Access Requirements: Yes	External User Access Requirements: CAL	Included Technologies: N/A
Notices: N/A		

3.1 Server Software Access

Base Access License	Project Server 2016 CAL Project Online Professional User SL	Project Online Essentials User SL Project Online Premium User SL

3.2 Additional Software

Software Development Kit		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: Project Server	Fail-Over Rights: N/A
License Mobility: Server licenses only	Migration Rights: N/A	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

SharePoint Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Office Audit and Control Management Server 2013	4/13	50	75	25				P	A	A	A
SharePoint Server 2016	5/16	50	75	25				P	A,SP	A	A
SharePoint Server 2016 Standard CAL (Device and User)	5/16	1	2	1				P		A	AO,ST
SharePoint Server 2016 Enterprise CAL (Device and User)	5/16	1	2	1				P	A	A	AO,ST

2. Product Conditions

Prior Version: SharePoint Server 2013 (10/12), no prior version for Microsoft Office Audit and Control Management Server	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): SharePoint Server	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Server/CAL	Product-Specific License Terms: Yes	Additional Software: Yes
Client Access Requirements: Yes	External User Access Requirements: Licensed with Server	Included Technologies: N/A
Notices: N/A		

3.1 Microsoft Audit and Control Management Server 2013 Server Software Access

Base Access License	SharePoint Server 2013 Standard CAL and SharePoint Server 2013 Enterprise CAL CAL Equivalent License (refer to Appendix A)	SharePoint Online Plan 2 User SL

3.2 SharePoint Server 2016 Server Software Access

Base Access License	SharePoint Server 2016 Standard CAL CAL Equivalent License (refer to Appendix A)	SharePoint Online Plan 1 or 2 User SL SharePoint Online Plan 2 User SL

3.2.1 Additional SharePoint Server Functionality Associated with SharePoint Enterprise CAL

Business Connectivity Services Line of Business Webparts; Office 2016 Business Connectivity Services Client Integration; Access Services; Enterprise Search; E-discovery and Compliance; InfoPath Forms Services; Excel Services, PowerPivot, and PowerView; Visio Services; PerformancePoint Services; Custom Analytics Reports; and Advanced Charting.

Additive Access License	SharePoint Server 2016 Enterprise CAL CAL Equivalent License (refer to Appendix A)	SharePoint Online Plan 2 User SL

3.3 CAL Waiver for Users Accessing Publicly Available Content

CALs are not required to access content, information, and applications that Customer makes publicly available to users over the Internet (i.e., where access is not restricted to Intranet or Extranet scenarios).

3.4 Additional Software

Software Development Kit		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: SharePoint Server and Office Audit and Control Management Server	Fail-Over Rights: N/A
License Mobility: SharePoint Server and Office Audit and Control Management Server (server licenses only)	Migration Rights: Product List - June 2015 (SharePoint Server and SharePoint Server for Internet Sites)	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Skype for Business Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Skype for Business Server 2015	5/15	50	75	25				P	A	A	A
Skype for Business Server 2015 Standard CAL (Device and User)	5/15	1	2	1				P		A	AO,ST
Skype for Business Server 2015 Enterprise CAL (Device and User)	5/15	1	2	1				P	A	A	AO,ST
Skype for Business Server 2015 Plus CAL (Device and User)	5/15	1	2	1				P	A, E	A	A,ST
Skype for Business Plus CAL (User SL)							UC	P	A,UC		

2. Product Conditions

Prior Version: Lync Server 2013 (10/12), Lync Server 2010 Standard and Enterprise (12/10)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Server/CAL	Product-Specific License Terms: N/A	Additional Software: Yes
Client Access Requirements: All editions	External User Access Requirements: Licensed with Server	Included Technologies: Windows Software Components
Notices: H.264/MPEG-4 and/or VC-1		

3.1 Server Software Access

Base Access License	Skype for Business Server 2015 Standard CAL Skype for Business Online Plan 1 G User SL Skype for Business Online Plan 2A User SL CAL Equivalent License (refer to Appendix A)	Skype for Business Online Plan 1 User SL Skype for Business Online Plan 2 User SL Skype for Business Online Plan 2G User SL

3.1.1 Additional Functionality Associated with Skype for Business Server Enterprise CAL

Audio, Video and Web Conferencing, Desktop Sharing, Room Systems and Multiple HD Video Streams

Additive Access License	Skype for Business Server 2015 Enterprise CAL Skype for Business Online Plan 2A User SL Live Meeting Standard User SL CAL Equivalent License (refer to Appendix A)	Skype for Business Online Plan 2 User SL Skype for Business Online Plan 2G User SL Live Meeting Professional User SL

3.1.2 Additional Functionality Associated with Skype for Business Server Plus CAL

Voice Telephony and Call Management

Additive Access License	Skype for Business Server 2015 Plus CAL Skype for Business Online Cloud PBX User SL	CAL Equivalent License (refer to Appendix A) Skype for Business Plus CAL User SL

3.2 Additional Software

Administrative Tools	Archiving and Monitoring Server Role	Audio/Video Conferencing Server Role
Autodiscovery Service Role	Central Management Server Role	Director Role
Edge Server Role	Skype for Business Web App Server Role	Mediation Server Role
Microsoft Lync Phone Edition	Microsoft Skype for Business Server 2015 Control Panel	Microsoft Lync Server 2013 Group Chat Administration Tool
Microsoft Lync Web App	Mobility Service Role	PowerShell Snap-in
Reach Application Sharing Server Role	Persistent Chat Server Role	Survivable Branch Appliance Role
Topology Builder	Unified Communications Application Server Role	Video Interop Server Role
Web Conferencing Server Role		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: Skype for Business Server	Fail-Over Rights: N/A
License Mobility: Server licenses only	Migration Rights: Product List - April 2015	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

R Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
R Server 2016 for Hadoop	1/16							P	A	A	A
R Server 2016 for Linux	1/16							P	A	A	A
R Server 2016 for Teradata DB	1/16							P	A	A	A

2. Product Conditions

Prior Version: N/A	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: Per Core Products only	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Per Core – Linux editions, Specialty Servers – Hadoop and Teradata DB editions	Product-Specific License Terms: Specialty Server editions	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: N/A
Notices: N/A		

3.1 R Server 2016 for Hadoop and R Server for Teradata DB

Each Server License for R Server 2016 for Hadoop and R Server 2016 for Teradata DB covers up to 24 cores on a [Licensed Server](#).

3.2 GNU Lesser General Public Licensed libraries

[Licensed User](#) may reverse engineer, decompile or disassemble the R Server software, or otherwise attempt to derive the source code for the R Server software (all editions) but only to the extent required to debug changes to any libraries licensed under the GNU Lesser General Public License that may be included with and linked to by the software.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: All editions	Fail-Over Rights: N/A
License Mobility: Yes	Migration Rights: N/A	Roaming Rights: N/A
Self Hosting: Yes	SA Equivalent Rights: Yes	

[Table of Contents](#) / [Glossary](#) / [Index](#)

SQL Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
SQL Server 2016 Standard	6/16	15	23	8				P	A,SP	A	A
SQL Server 2016 Standard Core (2-pack Core License)	6/16	50	75	25	OM			OM, P	A,SP	A	A
SQL Server 2016 Enterprise	6/16			38				P	A	A	A
SQL Server 2016 Enterprise Core (2-pack Core License)	6/16	125	188	63	OM			OM, P	A,SP	A	A
SQL Server 2016 CAL	6/16	1	2	1				P	A,SP	A	AO,ST

2. Product Conditions

Prior Version: SQL Server 2014 (4/14)	Product Pool: Server – All editions	Down Editions: Enterprise Core to Standard, Business Intelligence, Workgroup or Small Business or 2008 R2 Datacenter; Standard to Workgroup or Small Business
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: Per Core Products only	Reduction Eligible: N/A
Reduction Eligible (SCE): All editions	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

2.1 SQL Server 2016 Enterprise

New [Server](#) Licenses for SQL Server 2016 Enterprise (Server/CAL) are not available. Existing SA customers upgrading to the 2016 version should refer to the [June 2016 Product Terms](#) for their License Terms.

2.2 SQL Server Parallel Data Warehouse

SQL Server Parallel Data Warehouse is a deployment option for SQL Server 2016 Enterprise customers. Customers are eligible to use only the software builds made available during the term of their SA coverage.

2.3 SQL Server Parallel Data Warehouse Optional Build without Oracle Java

Customers may acquire a build of the product with Oracle Java or, upon request, without Oracle Java. For more information refer to <http://www.microsoft.com/en-us/sqlserver/solutions-technologies/data-warehousing/pdw.aspx>.

3. Use Rights

License Terms: Universal ; Server/CAL – Standard, Per Core – Standard Core and Enterprise Core	Product-Specific License Terms: All editions	Additional Software: All editions
Client Access Requirements: Server/CAL editions only	External User Access Requirements: CALs (Server/CAL editions only)	Included Technologies: Windows Software Components
Notices: N/A		

3.1 Server Software Access

Base Access License	SQL Server 2016 CAL

3.2 Automatic Updates to Previous Versions of SQL Server

If the software is installed on [Servers](#) or devices running any supported editions of SQL Server prior to SQL Server 2012 (or components of any of them) this software will automatically update and replace certain files or features within those editions with files from this software. This feature cannot be switched off. Removal of these files may cause errors in the software and the original files may not be recoverable. By installing this software on a [Server](#) or device that is running such editions you consent to these updates in all such editions and copies of SQL Server (including components of any of them) running on that [Server](#) or device.

3.3 Running Instances for Standard Edition

For each [Server](#) License, software may be run in only one [Physical OSE](#) or [Virtual OSE](#) at a time, but Customer may use any number of [Running Instances](#) of the server software in that [OSE](#).

3.4 Fail-Over Servers for Parallel Data Warehouse (PDW)

The PDW Appliance is a single unit made up of two or more compute nodes (Licensed Servers) all controlled by a single PDW control virtual machine ([Virtual OSE](#)). Technology is built in to the appliance which allows the software to fail-over to another compute node on the appliance. Customer does not need additional [Licenses](#) for the software running in fail-over [OSEs](#) as executed by the PDW Appliance technology.

3.5 Additional Software

3.5.1 Additional Software - All (except Parallel Data Warehouse)

Client Quality Connectivity	Client Tools Backwards Compatibility	Client Tools Connectivity
Client Tools SDK	Data Quality Client	Distributed Replay Client

Documentation Components	Management Tools - Basic	Management Tools - Complete
Reporting Services Add-in for SharePoint Products	SQL Client Connectivity SDK	

3.5.2 Additional Software - Parallel Data Warehouse

Parallel Data Warehouse Control Virtual Machine		

4. Software Assurance

SA Benefits: Server	Disaster Recovery: All editions	Fail-Over Rights: All editions (Not applicable to Parallel Data Warehouse)
License Mobility: All editions (Not applicable to Parallel Data Warehouse)	Migration Rights: SQL Server 2014 Business Intelligence and Parallel Data Warehouse (Section 4) Product List - March 2014 and June 2015	Roaming Rights: N/A
Self Hosting: All editions	SA Equivalent Rights: Yes	

4.1 SQL Server 2016 Enterprise Core - Unlimited Virtualization

Customer may run any number of instances of the server software in any number of **OSEs** on any **Licensed Server** for which it has full SA coverage on all of its core licenses for the **Server**.

4.2 SQL Server 2016 Enterprise Core - Parallel Data Warehouse Feature Updates

Customers with SA coverage are eligible for Parallel Data Warehouse feature releases (e.g., appliance updates) available between major product releases.

4.3 SQL Server Buy-Out Option under the Enrollment for Application Platform EAP

Customer may renew SA for SQL Server Enterprise Server/CAL **Licenses**, but the only buy-out option at the end of Customer's enrollment term will be for core **Licenses**.

[Table of Contents](#) / [Glossary](#) / [Index](#)

System Center

System Center Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
System Center 2016 Datacenter Server Management License (2-pack Core License)	10/16		13	8	OM			OM, P	A	A	A
System Center 2016 Standard Server Management License (2-pack Core License)	10/16		3	2	OM			OM, P	A	A	A

2. Product Conditions

Prior Version: System Center 2012 R2 (10/13)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Management Servers	Product-Specific License Terms: All editions	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: SQL Server Technology, Windows Software Components
Notices: Internet-based Features , Bing Maps		

3.1 Management License - System Center 2016 Standard

Server Management License	System Center 2016 Standard Management License

3.2 Management License - System Center 2016 Datacenter

Server Management License	System Center 2016 Datacenter Management License

3.3 SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software included in the Product in one [OSE](#) for the limited purpose of supporting that Product and any other Product that includes SQL Server database software.

3.4 Windows Server Containers

Customer may Manage any number of [OSEs](#) instantiated as [Windows Server Containers](#) on the [Licensed Server](#).

4. Software Assurance

SA Benefits : Server	Disaster Recovery : All editions	Fail-Over Rights: N/A
License Mobility : All editions (License Mobility through SA only)	Migration Rights : Product List - October 2013 , Product Terms - October 2016	Roaming Rights: N/A
Self Hosting : All editions	SA Equivalent Rights: N/A	

4.1 Nano Server

Customers with active SA on System Center Standard or Datacenter [Licenses](#) may Manage the Nano Server deployment option.

4.2 System Center Configuration Manager Current Branch Rights

Customers with active SA on System Center Standard or Datacenter [Licenses](#) may install and use the Current Branch option of System Center Configuration Manager.

4.3 System Center Global Service Monitor

Customers with active SA coverage for the [Management Licenses](#) may use System Center Global Service Monitor to monitor the web applications running on [OSEs](#) licensed with these [Management Licenses](#). Use of this Online Service is subject to the OST.

[Table of Contents](#) / [Glossary](#) / [Index](#)

System Center Configuration Manager

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
System Center Configuration Manager 1606 Client Management License per OSE	10/16		2	1				P		A	AO,ST
System Center Configuration Manager 1606 Client Management License per User	10/16		2	1				P		A	
System Center Configuration Manager 1606 Client Management License (Client ML) (Student Only)	10/16		2	1							

2. Product Conditions

Prior Version : System Center 2012 R2 Configuration Manager (10/13),	Product Pool : Server	Extended Term Eligible: N/A
Down Editions: N/A	Prerequisite: N/A	Prerequisite (SA) : Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms : Universal ; Management Servers	Product-Specific License Terms : Yes	Additional Software: N/A
Client Access Requirement: N/A	External User Access Requirement: N/A	Included Technologies : SQL Server Technology, Windows Software Components
Notices : Internet-based Features , Bing Maps		

3.1 Management License

Client Management License	System Center Configuration Manager 1606 (User or OSE)	Management License Equivalent License (refer to Appendix A)

Attachment E - Page 82 of 245

Microsoft Intune User SL

3.2 SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software included in the Product in one [OSE](#) only for the purpose of supporting that Product and any other Product that includes SQL Server database software.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: Yes	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - October 2013	Roaming Rights: N/A
Self Hosting: Yes	SA Equivalent Rights: N/A	

4.1 System Center Configuration Manager – VDI Rights

Customers with active SA coverage for System Center Configuration Manager CMLs, Core CALs, or Enterprise CALs (each, a “VDI qualifying license”) may use the software to manage, at any one time, up to four [Virtual OSEs](#) in which software used remotely from the device or by the user to which that VDI qualifying [License](#) has been assigned, is running. Each [Virtual OSE](#) may be run on a different virtual desktop infrastructure hosts.

4.2 System Center Configuration Manager Current Branch Rights

Customers with active SA on System Center Configuration Manager Licenses, or with equivalent subscription rights, may install and use the Current Branch option of System Center Configuration Manager.

[Table of Contents / Glossary / Index](#)

System Center Data Protection Manager

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
System Center 2016 Data Protection Manager per OSE (Client ML)	1/17	(1)	2	1				P	A	A	AO,ST
System Center 2016 Data Protection Manager per User (Client ML)	1/17		2	1				P	A	A	

2. Product Conditions

Prior Version : System Center Data Protection Manager component of System Center 2012 Client Management Suite (10/13)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA) : Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms : Universal ; Management Servers	Product-Specific License Terms : Yes	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies : SQL Server Technology, Windows Software Components
Notices : Internet-based Features , Bing Maps		

3.1 Management License

Client Management License	System Center 2016 Data Protection Manager License (User or OSE)

3.2 SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software included in the Product in one [OSE](#) for the limited purpose of supporting that Product and any other Product that includes SQL Server database software.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - October 2013	Roaming Rights: N/A

[Self Hosting](#): All editions

SA Equivalent Rights: N/A

4.1 Software Assurance Migration for Customers with System Center 2016 Client Management Suite

System Center 2016 Client Management Suite was the last version of Client Management Suite. Each component of Client Management Suite is now licensed as a separate product. For purposes of this section 4.1, "Eligible License" means a System Center 2016 Client Management Suite management [License](#) with SA obtained by Customer as of January 1, 2017 and any System Center 2016 Client Management Suite management [License](#) with SA subsequently obtained under the same agreement through a programmatic true-up. For each Eligible License, Customer is granted one System Center 2016 Data Protection Manager management [License](#), which will supersede and replace that Eligible License.

[Table of Contents](#) / [Glossary](#) / [Index](#)

System Center Endpoint Protection

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
System Center Endpoint Protection 1606 (Device and User SL)	10/16	1						P		A	A,ST

2. Product Conditions

Prior Version: System Center 2012 R2 Endpoint Protection (10/13)	Product Pool: Server	Extended Term Eligible: N/A
Down Editions: N/A	Prerequisite: N/A	Prerequisite (SA): N/A
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Management Servers	Product-Specific License Terms: Yes	Additional Software: N/A
Client Access Requirement: N/A	External User Access Requirement: N/A	Included Technologies: N/A
Notices: Internet-based Features		

3.1 Device and User SLs

Customer may purchase Device or User SLs to meet the Client Management License requirement under the [Management Servers License Model](#).

3.2 Server Management SLs

In addition to User SL requirements, Server Management Licenses are required for each Server in the number specified in the System Center 2016 Datacenter and Standard license terms. For purposes of this statement, [OSEs](#) running server operating systems that access System Center Endpoint Protection or related software are managed [OSEs](#). For this paragraph, a "Servers" is a device on which Customer runs server operating system software.

3.3 Substitution of Scan Engines

Microsoft may substitute comparable software and files for the Online Service's:

- anti-virus and anti-spam software; and
- signature files and content filtering data files.

4. Software Assurance

SA Benefits: N/A	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - March 2014	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

System Center Operations Manager

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES

System Center 2016 Operations Manager per OSE (Client ML)	1/17	(1)	2	1				P	A	A	AO,ST
System Center 2016 Operations Manager per User (Client ML)	1/17		2	1				P	A	A	

2. Product Conditions

Prior Version: System Center Operations Manager component of System Center 2012 Client Management Suite (10/13)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal; Management Servers	Product-Specific License Terms: Yes	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: SQL Server Technology, Windows Software Components
Notices: Internet-based Features , Bing Maps		

3.1 Management License

Client Management License	System Center 2016 Operations Manager License (User or OSE)

3.2 SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software included in the Product in one [OSE](#) for the limited purpose of supporting that Product and any other Product that includes SQL Server database software.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - October 2013	Roaming Rights: N/A
Self Hosting: All editions	SA Equivalent Rights: N/A	

4.1 Software Assurance Migration for Customers with System Center 2016 Client Management Suite

System Center 2016 Client Management Suite was the last version of Client Management Suite. Each component of Client Management Suite is now licensed as a separate product. For purposes of this section 4.1, "Eligible License" means a System Center 2016 Client Management Suite management [License](#) with SA obtained by Customer as of January 1, 2017 and any System Center 2016 Client Management Suite management [License](#) with SA subsequently obtained under the same agreement through a programmatic true-up. For each Eligible License, Customer is granted one System Center 2016 Operations Manager management [License](#), which will supersede and replace that Eligible License.

[Table of Contents](#) / [Glossary](#) / [Index](#)

System Center Orchestrator

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
System Center 2016 Orchestrator per OSE (Client ML)	1/17	(1)	2	1				P	A	A	AO,ST
System Center 2016 Orchestrator per User (Client ML)	1/17		2	1				P	A	A	

2. Product Conditions

Prior Version: System Center Orchestrator component of System Center 2012 Client Management Suite (10/13)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Management Servers	Product-Specific License Terms: Yes	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: SQL Server Technology, Windows Software Components
Notices: Internet-based Features , Bing Maps		

3.1 Management License

Client Management License	System Center 2016 Orchestrator License (User or OSE)

3.2 SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software included in the Product in one [OSE](#) for the limited purpose of supporting that Product and any other Product that includes SQL Server database software.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - October 2013	Roaming Rights: N/A
Self Hosting: All editions	SA Equivalent Rights: N/A	

4.1 Software Assurance Migration for Customers with System Center 2016 Client Management Suite

System Center 2016 Client Management Suite was the last version of Client Management Suite. Each component of Client Management Suite is now licensed as a separate product. For purposes of this section 4.1, “Eligible License” means a System Center 2016 Client Management Suite management [License](#) with SA obtained by Customer as of January 1, 2017 and any System Center 2016 Client Management Suite management [License](#) with SA subsequently obtained under the same agreement through a programmatic true-up. For each Eligible License, Customer is granted one System Center 2016 Orchestrator [License](#), which will supersede and replace that Eligible License.

[Table of Contents](#) / [Glossary](#) / [Index](#)

System Center Service Manager

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
System Center 2016 Service Manager per OSE (Client ML)	1/17	(1)	2	1				P	A	A	AO,ST
System Center 2016 Service Manager per User (Client ML)	1/17		2	1				P	A	A	

2. Product Conditions

Prior Version: System Center Service Manager component of System Center 2012 Client Management Suite (10/13)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Management Servers	Product-Specific License Terms: Yes	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: SQL Server Technology, Windows Software Components
Notices: Internet-based Features , Bing Maps		

3.1 Management License

Client Management License	System Center 2016 Service Manager License (User or OSE)

3.2 SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software included in the Product in one [OSE](#) for the limited purpose of supporting that Product and any other Product that includes SQL Server database software.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - October 2013	Roaming Rights: N/A
Self Hosting: All editions	SA Equivalent Rights: N/A	

4.1 Software Assurance Migration for Customers with System Center 2016 Client Management Suite

System Center 2016 Client Management Suite was the last version of Client Management Suite. Each component of Client Management Suite is now licensed as a separate product. For purposes of this section 4.1, "Eligible License" means a System Center 2016 Client Management Suite management [License](#) with SA obtained by Customer as of January 1, 2017 and any System Center 2016 Client Management Suite management [License](#) with SA subsequently obtained under the same agreement through a programmatic true-up. For each Eligible License, Customer is granted one System Center 2016 Service Manager management [License](#), which will supersede and replace that Eligible License.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Virtual Desktop Infrastructure (VDI) Suite

Customers looking for information about how to license and use the VDI Suite should refer to the April 2015 Product Use Rights <http://go.microsoft.com/?linkid=9839206> and June 2015 Product List <http://go.microsoft.com/?linkid=9839207>.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Visual Studio

Visual Studio

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Visual Studio Professional 2015	9/15	2									
Visual Studio Professional 2015 with MSDN	7/15	(1)	2	1	OM			OM, P	A, SP	A	A
Visual Studio Enterprise 2015 with MSDN	7/15	(1)	51	17	OM			OM, P	A, SP	A	A
Visual Studio Test Professional 2015 with MSDN	7/15	(1)	9	3	OM			OM, P	A, SP	A	A
MSDN Platforms	6/13	(1)	9	3	OM			OM, P	A, SP	A	A

2. Product Conditions

Prior Version: Visual Studio 2013 (10/13)	Product Pool: Applications	Down Editions: Enterprise to Professional
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): All	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

2.1 Visual Studio Premium 2013 with MSDN and Visual Studio Ultimate 2013 with MSDN

Visual Studio Enterprise 2015 with MSDN is the successor version to Visual Studio Premium 2013 with MSDN and Visual Studio Ultimate 2013 with MSDN.

2.2 License Grant for SQL Server Parallel Data Warehouse Developer

Each [Licensed User](#) of Visual Studio Professional with MSDN 2015, Visual Studio Enterprise 2015 with MSDN and Visual Studio Test Professional 2015 with MSDN is deemed to have one License for SQL Server 2012 Parallel Data Warehouse Developer.

2.3 License Grant for Visual Studio Team Foundation Server 2017

Each [Licensed User](#) of Visual Studio Professional 2015 with MSDN, Visual Studio Enterprise 2017 with MSDN, Visual Studio Test Professional 2015 with MSDN and MSDN Platforms is deemed to have one [Server](#) License for Visual Studio Team Foundation Server 2017 and one Team Foundation Server User CAL. The [CAL](#) is for the sole use of the [Licensed User](#).

2.4 Microsoft Azure Platform Services

Microsoft Azure benefits cannot be combined from multiple MSDN subscriptions onto a single Microsoft Azure account.

3. Use Rights

License Terms: Universal ; Developer Tools	Product-Specific License Terms: All	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: SQL Server Technology, Windows Software Components, Microsoft SharePoint, Windows SDK, Microsoft Office Components, Microsoft Advertising SDK
Notices: Internet-based Features – All, Bing Maps – All (except MSDN Platforms), H.264/MPEG-4 AVC and/or VC-1 – All (except MSDN Platforms)		

3.1 BUILDSEVER.TXT File

Customer may install copies of the files in the BuildServer Lists found at <http://go.microsoft.com/fwlink/?LinkId=286955> onto its build machines solely for the purpose of compiling, building, verifying and archiving its programs or to run quality or performance tests on its build machines as part of the build process.

3.2 Utilities

Customer may copy and install the Utilities listed at <http://go.microsoft.com/fwlink/?LinkId=286955> that Customer receives with the software on to Customer's other third party machines solely to debug and deploy Customer's programs and databases that Customer develops with the software. Customer must delete all the Utilities installed onto a device when it finishes debugging its program or 30 days after it installs them on that device, whichever comes first. Microsoft is not responsible for any third party use of or access to Utilities Customers installs on any device.

3.3 System Center – Virtual Machine Manager (SCVMM) – Visual Studio Enterprise with MSDN, and Visual Studio Test Professional with MSDN

Each licensed user of Visual Studio Enterprise with MSDN or Visual Studio Test Professional with MSDN may install and run SCVMM with the Visual Studio software for the purpose of creating, deploying and managing lab environment(s). A lab environment is a virtual operating system environment used solely for the purpose of developing and testing Customer's programs. Customer does not need Management Licenses for that use.

3.4 Office Professional Plus 2016 – Visual Studio Enterprise with MSDN

Each [Licensed User](#) of Visual Studio Enterprise with MSDN may also install and use one copy of Office Professional Plus 2016 on one device for production use. Except as provided here, the [Desktop Applications License Model](#) in the [License Terms](#) section applies to the [Licensed User's](#) use of this software.

3.5 GNU Lesser General Public Licensed libraries

[Licensed User](#) may reverse engineer, decompile or disassemble the Visual Studio software, or otherwise attempt to derive the source code for the Visual Studio software solely to the extent required to debug changes to any libraries licensed under the GNU Lesser General Public License that may be included with and linked to by the software.

4. Software Assurance

SA Benefits: Applications	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - March 2014 and Product Terms - September 2016	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: Yes	

4.1 Software Assurance Eligibility

Customers with expiring SA on any Visual Studio with MSDN License or an active retail subscription corresponding to the Visual Studio offerings in the Product Terms may renew coverage under any Visual Studio with MSDN license. When renewing to a different MSDN subscription level, the new use terms replace the prior use terms, and any software not included in the new MSDN subscription may no longer be used. Renewing into coverage that corresponds to a higher Visual Studio edition is facilitated through Step Up Licenses (refer [Appendix B – Software Assurance](#)).

4.2 MSDN Perpetual Rights

Customer's rights to use any software licensed through MSDN become perpetual when Customer's right to use Visual Studio becomes perpetual.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Visual Studio Team Foundation Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Visual Studio Team Foundation Server 2017 with SQL Server 2016 Technology	12/16		8	3				P	A,SP	A	A
Visual Studio Team Foundation Server 2017 CAL (Device and User)	12/16		8	3				P	A,SP	A	A

2. Product Conditions

Prior Version: Visual Studio Team Foundation Server 2015 (9/15)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: All	Prerequisite (SA): Appendix B
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): All	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Server/CAL	Product-Specific License Terms: All	Additional Software: All
Client Access Requirements: Yes	External User Access Requirements: CALs	Included Technologies: SQL Server Technology, Windows Software Components, Microsoft SharePoint Foundation 2013
Notices: N/A		

3.1 Server Software Access

Base Access License	Visual Studio Team Foundation Server 2017 CAL	Visual Studio Team Services paid user

3.1.1 Additional Functionality

Test Management

Additive Access License	Visual Studio Test Professional 2015 with MSDN MSDN Platforms	Visual Studio Enterprise 2015 with MSDN Visual Studio Team Services Test Manager Extension

3.1.2 Additional Functionality

Package Management

Additive Access License	Visual Studio Enterprise 2015 with MSDN	Visual Studio Team Services Package Management Extension

3.2 Usage Not Requiring CALs

The following uses do not require [CALs](#); view, edit, or enter work items; access Team Foundation Server Reporting; accessing Visual Studio Team Services via a Team Foundation Server 2017 Proxy; providing approvals to stages as part of the Release Management pipeline; and accessing Visual Studio Team Foundation Server through a pooled connection from another integrated application or service.

3.3 SQL Server Technology

Customer may run any number of [Instances](#) of any SQL Server database software included in the Product in one OSE for the limited purpose of supporting that Product and any other Product that includes SQL Server database software.

3.4 GNU Lesser General Public Licensed libraries

[Licensed User](#) may reverse engineer, decompile or disassemble the Visual Studio Team Foundation Server software, or otherwise attempt to derive the source code for the Visual Studio Team Foundation Server software solely to the extent required to debug changes to any libraries licensed under the GNU Lesser General Public License that may be included with and linked to by the software.

3.5 Visual Studio Team Foundation Server Build Services

If Customer has one or more [Licensed Users](#) of Visual Studio Enterprise with MSDN, Visual Studio Professional with MSDN, Visual Studio Enterprise (monthly or annual subscription), or Visual Studio Professional (monthly or annual subscription) then Customer may also install the Visual Studio software and permit access and use of it as part of Team Foundation Server 2017 Build Services by Customer's [Licensed Users](#) and [Licensed Devices](#) of Team Foundation Server 2017.

3.6 Release Management

Visual Studio Team Foundation Server includes one concurrent deployment using the Release Management feature. Each of the following provides one additional concurrent deployment per license:

- Visual Studio Enterprise 2015 with MSDN
- Visual Studio Enterprise (monthly or annual subscription)
- Team Services Build and Deployment Private Pipeline (paid instance)

3.7 Additional Software

Visual Studio Team Foundation Build Services	Visual Studio Team Foundation Server SharePoint Extensions	

4. Software Assurance

SA Benefits: Server	Disaster Recovery: Yes	Fail-Over Rights: N/A
License Mobility: Yes (server licenses only)	Migration Rights: Product Terms December 2016	Roaming Rights: N/A
Self Hosting: Yes	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Windows

Windows Desktop Operating System

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Windows 10 Pro Upgrade (Per Device)	8/15	2									
Windows 10 Enterprise LTSB 2016 Upgrade (Per Device)	10/16	2									
Windows 10 Enterprise E3 and LTSB 2016 Upgrade (Per Device)	10/16	(1)	3	1				E, P	E		
Windows 10 Enterprise E3 Per User (SL)	8/15	2							E		
Windows 10 Enterprise E3 Per User From SA (SL)	8/15	2							E		
Windows 10 Enterprise E5 Per Device or User (SL)	8/16	2							E		
Windows 10 Enterprise E5 Per User From SA (SL)	8/16	2							E		
Windows 10 Education Upgrade (Per Device)	8/15	(1)	3	1						ED	ED,SD,ST
Windows 10 Education E5 (Per Device)	8/16	(1)	3	1							ED
Windows 10 Education E5 Per Device Add-on (to E3 per device) (SL)	8/16	2									A
Windows 10 Mobile Enterprise (Per Device)	12/15	1									
Windows 8.1 Enterprise Sideload (Per Device)	11/13	1			OM						
Windows 10 Enterprise E3 Per User Add-on (to E3 per device) (SL)	12/14	2							E		A
Windows 10 Enterprise E5 Per Device or User Add-on (to E3 per device) (SL)	8/16	2							E		
Windows Virtual Desktop Access (Per Device SL)	7/07	2(1)						P	A, E	A	A
Windows Virtual Desktop Access Per User (SL)	12/14	2							E		
Windows Embedded 8 Standard Enterprise Kit (100 Pack)	10/13	2			OM						

2. Product Conditions

Prior Version: Windows 10 Enterprise LTSB (8/15), Windows Embedded 8.1 Industry (4/14)	Product Pool: System	Down Editions: Enterprise to Pro
Extended Term Eligible: N/A	Prerequisite: All licenses (except Virtual Desktop Access)	Prerequisite (SA): Appendix B, Section 4
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: Add-ons, Windows 10 Enterprise E5
Reduction Eligible (SCE): N/A	Student Use Benefit: Windows 10 Education E3	True-Up Eligible: N/A
UTD Discount: Windows 8.1 Enterprise		

2.1 Qualifying Operating Systems (OS)

Customers may purchase desktop operating system upgrade [Licenses](#) for Windows 10 Pro and/or Windows 10 Enterprise LTSC (“Windows 10 Enterprise”). The desktop operating system [Licenses](#) granted are upgrade [Licenses](#) only. Therefore, each device for which Customer acquires and on which it will run the Windows 10 Pro Upgrade or Windows 10 Enterprise Upgrade must be licensed to run one of the qualifying OS identified below. This requirement applies whether the upgrade [License](#) is purchased alone or together with SA.

2.1.1 Qualifying Operating Systems (OS) Chart

The qualifying OS by program type are:

Qualifying Operating Systems	New Enterprise Agreement (EA)/Open Value Company Wide (OV-OW) ¹	Existing Enterprise Agreement (EA)/Open Value Company Wide (OV-OW) ²	Microsoft Products and Services Agreement (MPSA)/Select Plus/Open ³	Microsoft Cloud Agreement	Academic and Charity
Windows 10					
Enterprise (N, KN) ⁴ Pro (N, KN)	X	X	X	X	X
Education, Home					X
Windows 8 and Windows 8.1					
Enterprise (N, K, KN), Pro (N, K, KN, diskless)	X	X	X		X
Windows 8 and Windows 8.1 (including Single Language)					X
Windows 7					
Enterprise (N, K, KN), Professional (N, K, KN, diskless, Ultimate)	X	X	X		X
Home Premium, Home Basic or Starter Edition					X
Windows Vista					
Enterprise (N, K, KN), Business (N, K, KN, Blade), Ultimate	X		X		X
Home Premium, Home Basic or Starter Edition					X
Windows XP					
Professional (N, K, KN, Blade), Tablet Edition (N, K, KN, Blade), XP Pro N, XP Pro Blade PC	X		X		X
Home and Starter Edition					X
Apple					
Apple Macintosh	X		X		X
Windows Embedded Operating Systems					
Windows 10 IoT Enterprise	X	X	X		X
Windows 2000 Professional for Embedded Systems	X		X		X
Windows XP Professional for Embedded Systems	X		X		X
Windows Vista Business for Embedded Systems, Ultimate for Embedded Systems	X		X		X
Windows 7 Professional for Embedded Systems, Ultimate for Embedded Systems	X	X	X		X
Windows Embedded 8/8.1 Pro, Industry Pro	X	X	X		X

¹ Also applicable to Qualified Devices acquired through merger or acquisition

² Column is also used to denote acceptable qualifying OS for a user's primary device when a user is licensed with Windows SA per User.

³ Does not apply to Academic, Charity, and OV-CW.

⁴ N, K, and KN are specialized editions available for certain markets.

⁵ See 2.1.2.1 below for use restrictions

2.1.2 Use Restricted Qualifying Operating Systems (OS) Chart

If the upgrade software is installed on devices running any of the qualifying OS listed below (the “Conditional Qualifying OS’s”), use restrictions apply and are detailed below the table in the Use Rights section. The use restrictions persist on devices licensed with Windows Software Assurance or Windows VDA notwithstanding any language in this document to the contrary.

Qualifying Operating Systems	New Enterprise Agreement (EA)/Open Value Company Wide (OV-OW) ¹	Existing Enterprise Agreement (EA)/Open Value Company Wide (OV-OW)	Microsoft Products and Services Agreement (MPSA)/Select Plus/Open ²	Academic and Charity
Windows 10 IoT Enterprise for Retail or Thin Clients ³	X		X	X
Windows Embedded 8 and 8.1 Industry Retail			X	X
Windows Embedded POSReady 7 Pro			X	X
Windows Embedded for Point of Service			X	X
Windows Embedded POSReady 2009			X	X

Windows Embedded POSReady 7			X	X
Windows XP Embedded			X	X
Windows Embedded Standard 7			X	X
Windows Embedded 2009			X	X
Windows Embedded 8 Standard			X	X

¹Also applicable to Qualified Devices acquired through merger or acquisition

²Does not apply to Academic, Charity, and OV-CW.

³Section 2.1.2.2 does not apply to Windows 10 IoT Enterprise for Retail or Thin Clients

2.1.2.1 Use restrictions for Conditional Qualifying Operating Systems

If the upgrade software is installed on devices licensed for and previously running any supported edition of a Conditional Qualifying OS, then the following conditions apply:

- **Specific Use.** Customer Licensed Device is designed for a specific use. Customer may only use the software for that use.
- **Other Software.** Customer may use other programs with the software as long as the other programs directly support the manufacturer's specific use for the device, or provide system utilities, resource management, or anti-virus or similar protection. If Customer's industry system performs desktop functions, then Customer must ensure that the desktop functions: (i) are only used to support the industry functionality, and (ii) operate only when technically integrated with the Industry Program or employ technically enforced policies or architecture to operate only when used with the Industry Program functionality. "Desktop functions," as used here, include: email, word processing, spreadsheets, database, scheduling or personal finance software. "Industry Program," as used here, means a device that only employs an industry or task-specific software program. The device may use terminal services protocols to access such software running on a server. Customer's industry system cannot be usable in its deployed configuration as a general purpose PC or as a commercial viable substitute for such a system.
- When upgrading from any version of Windows Embedded software that is designated "Point of Sale", "POS" or "Retail" in the table above, Customer must use the upgrade software with a POS application and the POS application must be the primary use of the software by each end user. A POS application is a software application which provides any of the following functions: process sales and service transactions, scan and track inventory, record or transmit customer information, perform related management functions, and provide information directly and indirectly to customers about available products and services.

2.1.2.2 Software Assurance Purchase restriction for Conditional Qualifying Operating Systems

Notwithstanding any contrary term in Section 4.1, SA may not be purchased for devices licensed with the Conditional Qualifying Operating Systems. This restriction does not apply to devices licensed with Windows 10 IoT for Retail or Thin Clients.

2.1.3 Qualifying OS Rules for Windows VL Upgrade Licenses

- The qualifying OS must be installed on the device to which the VL Upgrade License is to be assigned.
- Apple Macintosh is only a qualifying OS if it is preinstalled by the authorized manufacturer prior to the initial sale of the device.
- Customers must remove the qualifying OS from the device in order to deploy the VL Upgrade license, unless they also have SA on the VL Upgrade license.
- Academic Select, Academic Open, CASA, and Open Value Subscription – Education Solutions customers acquiring the upgrade License using Windows XP Starter Edition, Windows Vista Starter Edition or Windows 7 Starter Edition as a qualifying OS waive any right to transfer that License outside of the country of purchase.

2.2 Windows Enterprise Upgrade (version-less) and Windows Professional Upgrade (version-less)

Version-less Licenses for Windows Enterprise Upgrade and Windows Professional Upgrade are only available in the People's Republic of China under the Select Plus, Select, and Open License programs (two points). The Licenses are edition specific, so Customer must use a version of the edition of software acquired. The Qualifying Operating Systems for the Enterprise and Pro editions of Windows 10 apply, respectively, to the version-less Licenses for Windows Enterprise Upgrade and Windows Professional Upgrade.

2.3 Re-Imaging with Windows 10

If a third party intends to re-image Windows on Customer's separately Licensed Devices, Customer must first provide that third party with written documentation proving it has licenses for the software the third party will install.

2.4 Regional Fulfillment Options

2.4.1 N (Not with Windows Media Player) Versions of Microsoft Windows XP Professional, Vista Business and 7 Professional

Customers located in one of the countries established in the European Union (EU) or the European Free Trade Association (EFTA) may be eligible to acquire media for or download the N versions of Windows XP Professional, Windows Vista Business and Windows 7 Professional. Refer the March 2014 Product List for eligibility criteria and fulfillment details <http://go.microsoft.com/?linkid=9839207>.

2.4.2 K and KN Versions of Windows XP Professional, Vista Business and 7 Professional

Customers and their affiliates have specific Korea-specific media and download options for use of Windows XP Professional, Vista Business and 7 Professional in Korea. Refer the March 2014 Product List for requirements <http://go.microsoft.com/?linkid=9839207>.

2.4.3 Windows 8/8.1 Pro KN and Windows 10 Pro KN

Customers located in Korea who have an active volume licensing agreement or enrollment with Microsoft Operations Pte Ltd are eligible to acquire the media for Windows 8/8.1 Pro KN and Windows 10 Pro KN for deployment and use in Korea. No other use is permitted.

2.4.4 Windows 8/8.1 Pro N and Windows 10 Pro N (Not with Windows Media Player)

Customers with active agreements with Microsoft Ireland Operations Ltd are eligible to acquire the media for Microsoft Windows 8/8.1 Pro N and Windows 10 Pro N only for deployment and use in countries in the European Union (EU) or the European Free Trade Association (EFTA). (For purposes of Open License, an “active agreement” is one associated with an active Open License Authorization Number.)

2.5 Windows Embedded 8 Standard Enterprise Kit

Use of the software features enabled by the Windows Embedded 8 Standard Enterprise Kit is subject to the license terms for the underlying Windows Embedded 8 Standard software. The right to use the software features expires when the right to use the underlying software expires. The Windows Embedded 8 Standard Enterprise Kit License must be permanently assigned to a single device and may not be transferred to any other device.

2.6 Installation and Use Rights

For Customers licensed under a Microsoft Cloud Agreement:

- each user assigned a User SL may activate the software on up to five concurrent devices to run an instance of the software in the [Physical OSE](#); and
- Section 4 below does not apply.

3. Use Rights

License Terms: Universal ; Desktop Operating Systems, OST (Windows Defender Advanced Threat Protection portion of Windows 10 Enterprise E5)	Product-Specific License Terms: All Windows licenses	Additional Software: N/A
Client Access Requirements: N/A	External User Access Requirements: N/A	Included Technologies: N/A
Notices: H.264/MPEG-4 AVC and/or VC-1		

3.1 License Assignment

The assignment of [Licenses](#) for the desktop operating system (excluding Windows VDA) is permanent, except as provided in the Software Assurance section below. Refer to Section 4. Software Assurance for License reassignment rights for Windows SA and Windows VDA.

3.2 Windows Apps

Unless other terms are displayed to Customer or presented in the app’s settings, Customer agrees the services that it accesses from the Windows app is governed by the Microsoft Services Agreement at <http://go.microsoft.com/fwlink/?linkid=246338> or for Windows apps that access Xbox services, the Xbox.com terms of use at <http://xbox.com/legal/livetou>.

4. Software Assurance

SA Benefits: System	Disaster Recovery: N/A	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product List - June 2015 (Windows Companion Subscription)	Roaming Rights: February 2016 – Product Terms
Self Hosting: N/A	SA Equivalent Rights: N/A	

4.1 Windows 10 Enterprise E3/E5 (Per User and Per Device) and Windows Virtual Desktop Access (VDA) (Per User and Per Device) additional use rights granted via SA

“Software,” as used here, refers to Windows 10 Enterprise Current Branch or Windows Enterprise LTSB.

“Licensed Device,” as used here, refers to the device to which Customer assigns active coverage.

“Licensed User,” as used here, refers to the user to whom Customer assigns active coverage. If the underlying user License is transferred from one person to another, the original user of the License is no longer licensed.

- Any user of a Licensed Device, or any device used by a Licensed User, may remotely access up to four Instances of the Software Running in Virtual OSEs or one Instance of the Software Running in one Physical OSE on (a) device(s) dedicated to Customer’s use.
- Refer to sections 2.1.2.1 and 2.1.2.2 for use restrictions on Conditional Qualifying Operating System.
- Customer may create and store an Instance of the Software on one or two USB drives via Windows to Go and use them on Licensed Devices if licensed per device or on any device by users licensed per user.
- Customer may run Windows 10 Pro, or any earlier versions of the Software, in place of any Instance permitted in this section.
- Customer does not need a License to access its permitted Instances only to administer the Software.

The rights in the first column of the table apply to the licenses identified in the columns to the right, if there is a check in the cell associated with the licenses.

	Windows 10 Enterprise E3/E5	Windows VDA

	Device	User	Device	User
Customer may run up to four Instances in Virtual OSEs and one Instance in the Physical OSE locally on the Licensed Device . For Windows VDA (Per Device), this local use right applies only if the Licensed Device is also licensed for Windows 10/8.1 Pro or Enterprise, or Windows 7 Professional or Enterprise. If all of the Instances permitted to run in Virtual OSEs locally are used, Customer may use the Instance in the Physical OSE only to host and manage the Virtual OSEs .	X		X	
Customer may run up to four Instances in Virtual OSEs and one Instance in the Physical OSE locally on devices licensed for Windows 10/8.1 Pro or Enterprise, or Windows 7 Professional or Enterprise. If all of the Instances permitted to run in Virtual OSEs locally are used, then Customer may use the Instance in the Physical OSE only to host and manage the Virtual OSEs .		X		X
Customer may install the Software on Windows licensed devices with integrated screens 10.1" diagonally or less.		X		X

4.1.1 Windows 10 Enterprise Current Branch Rights

Windows 10 Enterprise Current Branch may only be used by Customers that have SA, Windows 10 Enterprise E3/E5, or VDA licenses.

Customers who allow SA to lapse must uninstall Windows 10 Enterprise Current Branch. Customers that have perpetual rights to Windows Enterprise may install the version of Windows Enterprise LTSB that is current at the time of lapse.

4.2 Qualifying Operating Systems (OS)

Each device for which Customer acquires SA and on which it will run the Windows 10 Enterprise Upgrade must be licensed to run one of the qualifying OS identified by program type in the Qualifying OS table in the Product Conditions section above.

- Customers who previously bought SA for Windows Pro may renew SA on their covered devices without the need to buy a Windows Enterprise Upgrade license.
- Customers who previously purchased Windows Pro Upgrade + SA may continue to purchase Pro Upgrade + SA until the end of their enrollment or agreement.

4.3 Windows Software Assurance Per Device Reassignment

Notwithstanding the License Assignment rules stated above, Customer may reassign Windows SA per device coverage with the associated Windows Enterprise Upgrade license from the original device to a replacement device, but not on a short-term basis (i.e., not within 90 days of the last assignment), as long as (1) Customer has licensed and installed on the replacement device the latest version of a Qualifying Operating System and Customer reassigns the underlying Windows Enterprise license to the same replacement device, and (2) Customer removes any related operating system upgrades from the original device. Reassignment of Windows Enterprise Upgrade licenses may only be done in conjunction with reassignment of Active Windows Software Assurance per Device coverage. Customer may reassign Windows VDA per Device licenses to another device in accordance with the terms and conditions generally applicable to device SLs in the "License Assignment and Reassignment" in the [Universal License Terms](#).

4.4 Windows 10 Enterprise Per User License Assignment Rules

4.4.1 Windows 10 Enterprise E3/E5 User SLs

The [Licensed User](#) must be the [Primary User](#) of at least one device licensed for Windows 10 Pro or Enterprise, Windows 8.1 Pro or Enterprise, or Windows 7 Professional or Enterprise. This one device must also be the Primary User's primary work device.

4.4.2 Windows 10 Enterprise E3/E5 User Add-ons

The [Licensed User](#) must be the [Primary User](#) of a device with either active Windows Desktop Operating System SA coverage or Windows VDA coverage.

4.5 Windows 10 Enterprise E3 and E5 Add-ons

Windows 10 Enterprise Add-ons are Subscription Licenses that

- are purchased in addition to (and associated with a device licensed for) either the Windows Desktop Operating System with SA coverage ("Qualifying Coverage") or VDA ("Qualifying License"), and
- expire upon the expiration of either the Qualified Coverage or Qualifying License.

For Windows 10 Enterprise Per User Add-ons, in addition to the above,

- Customer must assign the license to the Primary User of the Licensed Device (which must also be the Primary User's primary work device), and
- use of the Windows Enterprise software is subject to the Windows Enterprise per User License Terms or the VDA per User License Terms, associated with Qualifying Coverage or Qualifying License respectively.

Despite general License reassignment rights, these Add-on licenses may be reassigned only to Primary Users of other devices with either Qualifying Coverage or Qualifying Licenses. The Windows Desktop Operating System SA Per User Add-on may be purchased in any quantity up to the total number of SA and/or VDA licensed devices.

4.6 Enterprise Enrollments with combination Windows Per User and Per Device Windows SA or VDA coverage

Customers who wish to mix Windows SA per Device and Windows SA Per User licensing may do so as long as:

- All users who use unlicensed Qualified Devices are licensed with Windows SA per User (User SL or Add-on User SL), and
- All Qualified Devices used by unlicensed users are licensed with Windows SA per Device

4.7 Purchase Eligibility for Windows 10 Enterprise Per User From SA SLs

4.7.1 Enterprise Agreements

From SA User SLs may be purchased instead of SA for fully paid, perpetual Licenses with active SA for the Qualifying Products in the table below.

Qualifying Products	Corresponding from SA User SL
SA for the Windows Desktop Operating System	Windows 10 Enterprise E3 Per User From SA (SL) ¹
	Windows 10 Enterprise E5 Per User From SA ¹

¹ Available for purchase at enrollment anniversary or beginning of a new enrollment term only.

4.7.2 Enterprise Subscription Agreements

Subscription Licenses for Software Assurance for the Windows Desktop Operating System may be purchased at Customer's enrollment anniversary or the beginning of a new enrollment term with an ECS From SA User SL. The Subscription License must have been purchased at least three years prior to the purchase of the From SA User SL.

4.8 Microsoft Desktop Optimization Pack (MDOP)

Customer may install and use management functionality in the MDOP on Customer's other devices dedicated to their use to manage software on the Licensed Device or Licensed User's Devices. Customer may also use the AGPM, DaRT and UE-V to manage software on servers within its domain, so long as the desktops within that domain are licensed for MDOP use.

4.8.1 MDOP Eligibility

Customers with the following have rights to use MDOP and do not need to purchase MDOP separately.

- Windows Enterprise 10 E3/E5 per User SL;
- Windows 10 Enterprise E5 per Device SL;
- Windows 10 Enterprise VDA per User SL; or
- Agreement with an August 1, 2015, or later effective date and VDA per Device or Windows 10 Enterprise E3 per Device.

4.9 Academic Programs

The following applies to customers in all Academic Volume Licensing Programs:

4.9.1 Rights to Windows Enterprise LTSC

Academic Institutions with Windows 10 Enterprise E3/E5 or Windows 10 Education E3/E5 may install Windows 10 Enterprise LTSC in place of any permitted perpetual instance.

4.9.2 Rights to Windows 10 Enterprise, Windows 10 Education Edition, or Windows 10 Pro Education

Academic Institutions with Software Assurance for Windows Enterprise or Windows Education have rights to install and use Windows 10 Enterprise, Windows 10 Education, or Windows 10 Pro Education.

4.9.3 Downgrade Rights

Academic Institutions with Software Assurance for Windows Education have downgrade rights to Windows 8.1 Enterprise/Pro and previous versions of Windows 8.1 Enterprise/Pro, as well as, Windows Embedded 8.1 Industry and previous versions of Windows Embedded 8.1 Industry.

4.9.4 MDOP Eligibility

Academic Institutions with Software Assurance for Windows Enterprise or Windows Education have rights to install and use MDOP.

4.9.5 Windows To Go Student Option

Academic Institutions electing the Student Option are permitted a maximum of one Windows To Go Instance per licensed student device while that student is enrolled at the institution.

4.10 Windows 10 Mobile Enterprise

Customers with active Windows SA per User SL or per User Add-on may install and use Windows 10 Mobile Enterprise on secondary devices of each licensed user.

4.11 Windows Desktop Operating System – Rights to run “Clustered HPC Applications”

Customer may permit simultaneous use of the software on a [Licensed Device](#) used as a [Cycle Harvesting Node](#) to run [Clustered HPC Applications](#), as long as the [Licensed Device](#) is not used as a general purpose [Server](#), database [Server](#), web [Server](#), e-mail [Server](#), print [Server](#) or file [Server](#), for other multi-user access purposes, or for any other similar resource sharing purpose.

4.12 Windows Desktop Operating System – Windows Thin PC

Customer may use the Windows Thin PC software in place of Windows Desktop Operating System software but only to run the types of applications listed below.

- security
- management
- terminal emulation

- Remote Desktop and similar technologies
- web browser
- media player
- instant messaging client
- document viewers
- NET Framework and Java Virtual Machine

Customer may use the software on a device other than the one on which it was first installed if it moves the corresponding Software Assurance coverage to that other device.

4.13 Software Assurance for Windows Embedded Industry Enterprise

Customers with Software Assurance for Windows Embedded Industry Enterprise have the same rights and restrictions as Windows Software Assurance.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Windows Server

Windows MultiPoint Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Windows MultiPoint Server 2016 Premium	10/16	10	15	5				A		A	A

2. Product Conditions

Prior Version: Windows MultiPoint Server 2012 (12/12)	Product Pool: Server	Down Editions: N/A
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): N/A
Promotions: N/A	Qualified User Exemption: N/A	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Server/CAL	Product-Specific License Terms: All editions	Additional Software: All editions
Client Access Requirements: All editions	External User Access Requirements: CAL	Included Technologies: N/A
Notices: Internet-based Features , H.264/MPEG-4 AVC and/or VC-1		

3.1 Server Software Access

Base Access License	Windows Server 2016 Remote Desktop Services CAL and Windows Server 2016 CAL	Windows Server 2016 Remote Desktop Services CAL and CAL Equivalent License (refer to Appendix A)

3.1.1 Additional Functionality Associated with Windows Server 2016 Active Directory Rights Management Services CAL

Windows Server 2016 Rights Management Services

Additive Access License	Windows Server 2016 Active Directory Rights Management Services CAL	CAL Equivalent License (refer to Appendix A)

3.2 Running Instances of the Software

Customer may run on the [Licensed Server](#) at any one time one [Instance](#) of the server software in each of the [Physical OSE](#) and one [Virtual OSE](#). If Customer uses the server software in a [Virtual OSE](#), then server software used in the [Physical OSE](#) may be used only to host and manage the [Virtual OSE](#).

3.3 Access Licenses

[CALs](#) are not required for access in a [Physical OSE](#) that is used solely for hosting and managing [Virtual OSEs](#).

3.4 Windows MultiPoint Server 2016 Connector

Customer may install and use the Windows Server 2016 MultiPoint Connector software on any device that is licensed to access Windows Server 2016. It may use this software only to access the MultiPoint Server software. If it accesses the server software from this device solely to use the MultiPoint Dashboard it does not need a Remote Desktop Services CAL.

3.5 Installation Type

Customer may only install Remote Desktop Services and deploy and use the MultiPoint Services role.

3.6 Additional Software

For a list of Additional Software refer <http://go.microsoft.com/fwlink/?LinkId=245856>.

4. Software Assurance

SA Benefits: Server	Disaster Recovery: All editions	Fail-Over Rights: N/A
License Mobility: N/A	Migration Rights: Product Term - October 2016	Roaming Rights: N/A
Self Hosting: N/A	SA Equivalent Rights: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Windows Server

1. Program Availability

Products	DA	L	L/SA	SA	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Windows Server 2016 Active Directory Rights Management Services CAL	10/16	1	2	1				P	A	A	AO,ST
Windows Server 2016 CAL	10/16	1	2	1				P		A	AO,ST
Windows Server 2016 Remote Desktop Services CAL (Device and User)	10/16	1	2	1				P	A	A	A, AO,ST
Windows Server 2016 Remote Desktop Services External Connector	10/16	75	113	38	OM			OM, P	A	A	A
Windows Server 2016 Datacenter (2-pack Core License)	10/16	10	25	15	OM			OM, P	A	A	A
Windows Server 2016 Essentials	10/16	5	10	5				P		A	A
Windows Server 2016 Standard (2-pack Core License)	10/16	1	3	2				P	A	A	A
Windows Server 2016 Active Directory Rights Management Services External Connector	10/16	125	188	63	OM			OM, P	A	A	A
Windows Server 2016 External Connector	10/16	25	38	13	OM			OM, P	A	A	A

2. Product Conditions

Prior Version: Windows Server 2012 R2 (10/13), Windows Server 2012 for CALs and External Connectors (8/12)	Product Pool: Server	Down Editions: Datacenter or Standard to Windows Server 2008 R2 Enterprise, Standard, Essentials, Web, and HPC editions, or Essentials 2012 or 2012 R2
Extended Term Eligible: N/A	Prerequisite: N/A	Prerequisite (SA): N/A
Promotions: N/A	Qualified User Exemption: External Connectors	Reduction Eligible: N/A
Reduction Eligible (SCE): N/A	Student Use Benefit: N/A	True-Up Eligible: N/A
UTD Discount: N/A		

3. Use Rights

License Terms: Universal ; Per Core/CAL – All editions (except Essentials), Specialty Servers – Essentials	Product-Specific License Terms: All editions	Additional Software: All editions
Client Access Requirements: All editions (except Essentials)	External User Access Requirements: CALs or External Connector	Included Technologies: N/A
Notices: Internet-based Features , H.264/MPEG-4 AVC and/or VC-1		

3.1 Server Software Access

Base Access License	Windows Server 2016 CAL	CAL Equivalent License (refer to Appendix A)

3.1.1 Additional Functionality Associated with Windows Server 2016 Remote Desktop Services CAL

Microsoft Application Virtualization for Remote Desktop Services and Windows Server 2016 Remote Desktop Services functionality

Additive Access License	Windows Server 2016 Remote Desktop Services CAL	Windows Server 2016 Remote Desktop Services User SL

*Also required for use of Windows Server to host a graphical user interface (using the Windows Server 2016 Remote Desktop Services functionality or other technology).

3.1.2 Additional Functionality Associated with Windows Server 2016 Rights Management Services CAL

Windows Server 2016 Rights Management Services

Additive Access License	Windows Server 2016 Active Directory Rights Management Services CAL	Azure Information Protection (P1 and P2) User SL CAL Equivalent License (refer to Appendix A)

3.1.3 Additional Functionality Associated with Microsoft Identity Manager User CAL

Microsoft Identity Manager 2016 functionality

Additive Access License	Microsoft Identity Manager 2016 User CAL CAL Equivalent License (refer to Appendix A)	Azure Active Directory Premium (P1 and P2) User SL

*Also required for any person for whom the software issues or manages identity information.

3.1.4 Synchronization Service

Microsoft Identity Manager 2016 CALs not required for users only using Microsoft Identity Manager synchronization service.

3.2 Server External User Access

Base Access License	Windows Server 2016 External Connector

3.2.1 Additional Functionality Associated with Windows Server 2016 Remote Desktop Services External Connector License

Microsoft Application Virtualization for Remote Desktop Services and Windows Server 2016 Remote Desktop Services functionality

Additive Access License	Windows Server 2016 Remote Desktop Services External Connector

*Also required for use of Windows Server to host a graphical user interface (using the Windows Server 2016 Remote Desktop Services functionality or other technology).

3.2.2 Additional Functionality Associated with Windows Server 2016 Rights Management Services External Connector License

Windows Server 2016 Rights Management Services

Additive Access License	Windows Server 2016 Active Directory Rights Management Services External Connector

3.2.3 Additional Functionality Associated with Microsoft Identity Manager External Connector License

Microsoft Identity Manager 2016 functionality

Additive Access License	Microsoft Identity Manager 2016 External Connector

*Also required for any External User for whom the software issues or manages identity information (in absence of Microsoft Identity Manager 2016 CALs).

3.3 Additional Terms for Windows Server 2016 Essentials

3.3.1 Limitations on Use

- At any one time, Customer may use a [Running Instance](#) of the server software in each of the [Physical OSE](#) and in one [Virtual OSE](#).
- Customer must run the server software within a domain where the Server's Active Directory is configured as (i) the domain controller (a single server which contains all the flexible single master operations (FSMO) roles), (ii) the root of the domain forest, (iii) not to be a child domain, and (iv) to have no trust relationship with any other domains. If the server software is used in a [Virtual OSE](#), the Instance in the [Physical OSE](#) may be used only to run hardware virtualization software, provide hardware virtualization services, or run software to manage and service [Operating System Environment](#) on the [Licensed Server](#). That Instance does not need to meet the requirements in (i) through (iv) above.

3.3.2 Using the Server Software

A User Account is a unique user name with its associated password created through the Windows Server 2016 Essentials Console. Customer may use up to 25 user accounts. Each user account permits a named user to access and use the server software on that server. It may reassign a user account from one user to another provided that the reassignment does not occur within 90 days of the last assignment.

3.3.3 Windows Server 2016 Essentials Connector

Customer may install and use the Windows Server 2016 Essentials Connector software on no more than 50 devices at any one time. It may use this software only with the server software.

3.3.4 Windows Server 2016 Active Directory Rights Management Services Access

Customer must acquire a Windows Server 2016 Active Directory Rights Management Services CAL for each User Account through which a user directly or indirectly accesses the Windows Server 2016 Active Directory Rights Management Services functionality.

3.4 Windows Server Containers with Windows Server 2016 Standard and Datacenter

Customer may use any number of [OSEs](#) instantiated as [Windows Server Containers](#) on the [Licensed Server](#).

3.5 Additional Software for Windows Server 2016

AD Migration Tool	GBUNIECN.EXE Utility	

4. Software Assurance

SA Benefits : Server	Disaster Recovery : All editions	Fail-Over Rights: N/A
License Mobility : External Connector only	Migration Rights : Refer Product List - October 2013 and March 2014 (prior versions as well as HPC Pack, Windows HPC Server, Windows Server Enterprise, Windows Server HPC Edition, Windows Server for Itanium Based Systems, Windows Small Business Server); Product List - June 2015 (Forefront Identity Manager 2010 R2); Product Terms - October 2016	Roaming Rights: N/A
Self Hosting : All editions (except Essentials)	SA Equivalent Rights: N/A	

4.1 Microsoft Azure Hybrid Use Benefit

Refer to [Section 7. Microsoft Azure Hybrid Use Benefit](#) of the Microsoft Azure Product Entry for deploying Windows Server images on Microsoft Azure.

4.2 Nano Server

Customers with active SA on either Windows Server Standard or Datacenter [Licenses](#), Windows Server Base Access [Licenses](#), and Windows Server Additive Access [Licenses](#) may install and use the Nano Server deployment option. Active SA is also required on the Base Access License and Additive Access License.

4.3 Remote Desktop Services (“RDS”) User CAL and User SL – Extended Rights

Customer may use its RDS User CALs and User SLs with Windows Server software running in [OSEs](#) dedicated to its internal use on either Microsoft Azure Platform Services or the shared servers of a [License Mobility through Software Assurance Partner](#) for which it has completed and submitted the License Mobility Validation form. Other than administrative access by Customer’s [License Mobility through Software Assurance Partner](#), no other party may access the [OSE\(s\)](#). For any [CAL](#) or User SL Customer has used in this manner, it may later move to Microsoft Azure Platform Services or a new [License Mobility through Software Assurance Partner](#), but not sooner than 90 days after it initiated use in the environment it is leaving.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Online Services

Customer's purchase and use of Microsoft Online Services are governed by the Product Terms and the Microsoft Online Services Terms (OST) located at <http://go.microsoft.com/?linkid=9840733> and incorporated herein by reference.

Online Services Regional Availability

Visit <http://www.microsoft.com/online/faq.aspx#international> for a list of countries and regions in which the Online Services are available.

Online Services Purchasing Rules

The following purchasing rules apply to purchasing Online Services:

- Subscription terms vary by purchasing program. Under the Enterprise Agreement program, the subscription terms for Online Services other than Microsoft Azure must be coterminous, ending on the date of Customer's Enrollment end date.
- If Customer makes additional purchases of an Online Service, the end of the subscription term of the additional purchase must align with Customer's existing subscription term for the same Online Service.
- Customer may not reduce the number of users or devices covered by its Online Services subscription during the term of their Online Services subscription except as permitted in Customer's volume licensing agreement.
- Terms for Microsoft Azure are provided in the Microsoft Azure Product Entry.
- **Add-on** and **Step-up** User SLs must be purchased under the same volume licensing agreement and enrollment (if any) as their Qualifying License or base User SL. **Add-ons** expire upon the earlier of the expiration of the SA coverage for the Qualifying License or the **Add-on** User SL. **Step-ups** expire upon the earlier of the expiration of the **Step-up** User SL or base User SL.

Online Services Renewal

Online Services with Auto-Renewal will automatically renew the day after their subscription term expires, unless Customer chooses not to renew by opting out of auto-renewal at least of 30 days before the subscription expires by placing an order with their reseller or using a form that is available at <http://microsoft.com/licensing/contracts>. Online services subscriptions for government and academic customers will not be automatically renewed unless Customer chooses the auto-renewal option.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Azure Services

1. Definitions

Allocated Annual Commitment means the portion of the Monetary Commitment allocated annually through the Enrollment term.

Consumption Allowance is equal to fifty percent of the Allocated Annual Commitment. For example, for an Allocated Annual Commitment of \$100,000, the Consumption Allowance for that year would be \$50,000.

Consumption Rates means the prices for Microsoft Azure Services or, for certain Microsoft Azure Service Plans, any usage in excess of a specified quantity. Consumption Rates may also be referred to as "Overage Rates" or "Overage" in other Microsoft or Microsoft Azure documents.

Microsoft Azure Services Plan means a subscription to one of the individual Microsoft Azure Services identified below as a Microsoft Azure Services Plan. Services purchased as a Microsoft Azure Services Plan are not eligible for the Hosting Exception in the Online Services Terms.

Monetary Commitment means the total monetary amount a customer commits to pay over the term of the subscription for its use of eligible Microsoft Azure Services.

2. Subscription Term

Customers may only subscribe to Microsoft Azure Services (including Microsoft Azure Services Plans) for a subscription term that ends on the end date of Customer's Enrollment ("coterminous"). Customers must have at least two months remaining in their Enrollment term in order to subscribe to Microsoft Azure Services.

3. Purchasing Services

Microsoft Azure Services may be purchased in one or a combination of the following ways:

- Commitment:** Monetary Commitments are allocated proportionally through the Enrollment term. Customers may increase their Monetary Commitment at any time by placing additional orders. When an additional order is placed, Allocated Annual Commitment will be increased for that year by the amount of the order. For each subsequent year remaining in the Enrollment term, Allocated Annual Commitments will be increased by the amount of the additional order, multiplied by twelve, divided by the number of full months between when the additional order was placed and the anniversary date following the additional order.
 - Customers may reduce their Monetary Commitment for any future Enrollment anniversary by notifying their reseller, who must process the reduction with Microsoft prior to the Enrollment anniversary date.
 - Customers must consume their Allocated Annual Commitment by the last day of the month preceding the Enrollment anniversary each year, after which any unused portion of the Allocated Annual Commitment will be forfeited. Customers may utilize their annual

Attachment E - Page 100 of 245

Consumption Allowance by the last day of the month preceding the Enrollment anniversary each year, after which any unused portion of that Consumption Allowance will be forfeited.

- B. **Consumption:** Customers pay based on the amount of Microsoft Azure Services consumed during a billing period. Certain features of the Microsoft Azure Services may only be available for purchase on a consumption basis.
- C. **Microsoft Azure Services Plan:** Customers may be able to subscribe to a Microsoft Azure Service as a Microsoft Azure Services Plan.
- D. **Automatic Provisioning:** As part of the Server and Cloud Enrollment, Customers who have not ordered Microsoft Azure Services as part of their Enrollment may receive an activation email from Microsoft inviting them to provision Microsoft Azure Services under their Enrollment without a Monetary Commitment.

4. Pricing

If Customer does not have an Enterprise Enrollment, Enterprise Subscription Enrollment, Select Agreement, Select Plus Agreement or Server Cloud Enrollment, price level A will apply.

Microsoft may offer lower prices to Customer or Customer's reseller for individual Microsoft Azure Services during a Customer's Enrollment term on a permanent or temporary (promotional) basis.

5. Payment and Fees

Customers who have provisioned Microsoft Azure Services without a Monetary Commitment will be invoiced quarterly at Consumption Rates.

For Customers with a Monetary Commitment the first Allocated Annual Commitment will be invoiced immediately and future Allocated Annual Commitments will be invoiced on the anniversary of the Enrollment effective date. Alternatively, Customers may choose to pay their entire Monetary Commitment upon placing the initial order.

Each month, Microsoft will deduct from the Allocated Annual Commitment the monetary value of Customer's usage of eligible Microsoft Azure Services. Once Customer's Allocated Annual Commitment balance has been exhausted, any additional usage will be invoiced at Consumption Rates.

If a direct Enterprise Agreement Customer's usage is lower than the Allocated Annual Commitment plus the Consumption Allowance, any usage exceeding the Allocated Annual Commitment will be invoiced at the Consumption Rates to the Customer or its reseller on the anniversary of the Enrollment effective date for Years 1 and 2 and at the end of the subscription term for Year 3.

If a direct Enterprise Agreement Customer's usage is higher than the Allocated Annual Commitment plus the Consumption Allowance, all usage exceeding the Allocated Annual Commitment will be invoiced at Consumption Rates to the Customer or its reseller at the end of each Enrollment quarter.

For indirect Enterprise Agreement Customers, all usage exceeding the Allocated Annual Commitment will be invoiced at Consumption Rates to the Customer's reseller at the end of each Enrollment quarter.

All usage of the Microsoft Azure Services after the expiration or termination of Customer's subscription term will be invoiced to the customer or its reseller at then-current Consumption Rates on a quarterly basis.

The purchase of a Microsoft Azure Services Plan will be invoiced to Customer or its reseller according to the terms of Customer's volume licensing agreement governing payment terms for the order of Online Services generally. Monetary Commitment cannot be applied to the purchase of a Microsoft Azure Plan; provided, however, that if a Microsoft Azure Services Plan includes the purchase of an initial quantity of a service ("Initial Quantity"), Customer usage that exceeds the Initial Quantity will be billed at Consumption Rates, and Customer's Allocated Annual Commitment can be applied to such usage.

6. Open License, Open Value and Open Value Subscription Programs

6.1 Definitions

Consumption Rates mean for purposes of the Open License, Open Value and Open Value Subscription agreements, prices for all Microsoft Azure Services.

Portal means the online portal through which Customer administers its Subscription.

Subscription means a subscription with a value set at time of order that can be redeemed for a quantity of Microsoft Azure Services.

6.2 Subscription Term

The Subscription period starts at the time of product key redemption and not the time of order. Once the product key is redeemed, Microsoft will not accept return requests submitted by Microsoft's partners. Subscriptions are valid for the earlier of 12 months or until the value is consumed. Subscriptions may not be combined. Customer may have multiple active Subscriptions. New Subscriptions can be purchased at any time.

7. Microsoft Azure Hybrid Use Benefit

Under the Microsoft Azure Hybrid Use Benefit ("HUB"), a customer with Windows Server Licenses covered with SA may upload to and use its own Windows Server image on Microsoft Azure.

Azure HUB enables Customers' use of Windows Server on Microsoft Azure through Azure Virtual Machines ("Base Instances"). HUB does not include the cost of Base Instances, and Base instances do not include Windows Server. Each Windows Server processor [License](#) with SA, and each set of 16 Windows Server core [Licenses](#) with SA, entitles Customer to use Windows Server on Microsoft Azure on up to 16 [Virtual Cores](#) allocated across two or fewer Azure Base Instances. Each additional set of 8 core [Licenses](#) with SA entitles use on up to 8 [Virtual Cores](#) and one Base Instance.

Customer must indicate that it is using Windows Server under the HUB when configuring the uploaded image(s) on Azure. Customer may use its uploaded image(s) subject to the [Online Services Terms](#).

The HUB provides additive rights to deploy and use the software when exercised in connection with Datacenter [Licenses](#) and alternative rights when exercised in connection with Standard [Licenses](#). Standard [Licenses](#) are deemed "assigned to Azure" when Customer uses Windows Server under the HUB, and are subject to the [License](#) reassignment limitations in the [Universal License Terms](#).

Microsoft Azure Services

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Azure Services	1	OM			A	A	A	A

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: Until canceled
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: Allocated Annual Commitment	Reduction Eligible (SCE): Allocated Annual Commitment
Student Use Benefit: N/A	True-up Eligible: N/A	

2.1 Microsoft Azure Services Plans

If subscribed to by Customer as a Microsoft Azure Services Plan, individual Microsoft Azure Services may have different program availability or be subject to different terms. See the Microsoft Azure Services Plan-Specific entries below for more details.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Azure Plans

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Azure Active Directory Basic (User SL)	1					A		A,ST
Azure Active Directory Premium Plan 1 (User SL)	1	OM				A		A,ST
Azure Active Directory Premium Plan 2 (User SL)	1	OM			P	A		A
Azure Active Standard Support						A		A
Azure Active Professional Direct Support						A		A
Azure App Service Plan						A		
Azure Information Protection Premium Plan 1 (User SL)	1	OM			P	A	A	A,ST
Azure Information Protection Premium Plan 1 Add-on (User SL)						A		
Azure Information Protection Premium Plan 2 (User SL)		OM			P	A	A	A,ST
Azure Information Protection Premium Plan 2 Add-on (User SL)						A		
IoT Suite Predictive Maintenance Plan 1	1					A		A
IoT Suite Predictive Maintenance Plan 2	1					A		A
IoT Suite Remote Monitoring Plan 1						A		A
IoT Suite Remote Monitoring Plan 2						A		A
Azure Site Recovery (to Customer Owned Site)						A		A
Microsoft Azure StorSimple Plan with Device (8100 device)						A		A
Microsoft Azure StorSimple Plan with Device (8600 device)						A		A
Microsoft Azure StorSimple Plan 8100 Renewal (no device)						A		A
Microsoft Azure StorSimple Plan 8600 Renewal (no device)						A		A
Microsoft Azure StorSimple Standard Support						A		A
Microsoft Azure StorSimple Standard Support to Premium Support						A		A
Microsoft Azure StorSimple Premium Support						A		A
Microsoft Cloud App Security (User SL)	1	OM			P	A	A	A,ST

Microsoft Cloud App Security K (User SL)					A		
Microsoft MultiFactor Authentication	1			P	A	A	A,ST
Operations Management and Security E1 Add-on	1				A		A
Operations Management and Security E2 Add-on	1				A		A
Operations Management and Security E1					A		A
Operations Management and Security E1 From SA					A		A
Operations Management and Security E2					A		A
Operations Management and Security E2 From SA					A		A
Operations Management and Security: Insights and Analytics					A		A
Operations Management and Security: Automation and Control					A		A
Operations Management and Security: Security and Compliance					A		A
Operations Management and Security: Backup and Disaster Recovery					A		A

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: Operations Management and Security	Promotions: N/A
Qualified User Exemption: Microsoft Cloud App Security	Reduction Eligible: All (except Azure Active Support)	Reduction Eligible (SCE): All (except Azure Active Support, Azure RemoteApp)
Student Use Benefit: Microsoft Cloud App Security	True-Up Eligible: Azure Active Directory, Azure Information Protection Premium, Microsoft Cloud App Security, Microsoft MultiFactor Authentication, Operations Management and Security	

2.1 Operations Management and Security

2.1.1 Add-on SLs

For each Qualifying License Customer may purchase a combination of Add-ons, provided the total quantity does not exceed the Eligible Quantity in the table below.

Qualifying License(s) ¹	Add-on SL	Eligible Quantity
Core Infrastructure Server Suite Standard (2-pack Core License) System Center Standard (2-pack Core License)	Operations Management and Security E1 Add-on Operations Management and Security E2 Add-on	1/4 ²
Core Infrastructure Server Suite Datacenter (2-pack Core License) System Center Datacenter (2-pack Core License)	Operations Management and Security E1 Add-on Operations Management and Security E2 Add-on	1
Core Infrastructure Server Suite Standard (2 processor) System Center Standard (2 processor)	Operations Management and Security E1 Add-on Operations Management and Security E2 Add-on	2
Core Infrastructure Server Suite Datacenter (2 processor) System Center Datacenter (2 processor)	Operations Management and Security E1 Add-on Operations Management and Security E2 Add-on	8

¹Each Qualifying License must have active SA

²Requires a minimum of four Qualifying Licenses

2.1.2 Add-on SLs purchased under a different volume license agreement than the Qualifying License

An Operations Management and Security Add-on SL may be purchased under a different volume licensing agreement than its Qualifying License. If the SA coverage for the Qualifying License expires before the Operations Management and Security Add-on SL, the Operations Management and Security Add-on SL will expire at its next enrollment anniversary.

2.1.3 Software Included with Operations Management and Security E1/E2

During the term of each Operations Management and Security E1/E2 subscription, Customer may install and run one copy of the corresponding included software for Managing an OSE in Customer's own facility or in Microsoft Azure.

Operations Management and Security Subscription	Included Software
Operations Management and Security E1 Operations Management and Security E1 From SA	System Center Server Standard
Operations Management and Security E2 Operations Management and Security E2 from SA	System Center Server Standard
Operations Management and Security: Insights and Analytics	System Center Operation Manager
Operations Management and Security: Automation and Control	System Center Configuration Manager System Center Orchestrator System Center Service Manager
Operations Management and Security: Backup and Disaster Recovery	System Center Data Protection Manager System Center Virtual Machine Manager

2.1.4 From SA Purchasing Eligibility

From SA Subscription Licenses may be purchased instead of SA for fully paid, perpetual Licenses with active SA for the Qualifying Products in the table below. For each Qualifying Product, customer may purchase a combination of From SA SLs, provided the total quantity does not exceed the listed Eligible Quantity.

Qualifying Product	Corresponding From SA Subscription License	Eligible Quantity
Core Infrastructure Server Suite Standard (2-pack Core License) System Center Standard (2-pack Core License)	Operations Management and Security E1 From SA Operations Management and Security E2 From SA	1/4 ¹
Core Infrastructure Server Suite Datacenter (2-pack Core License) System Center Datacenter (2-pack Core License)	Operations Management and Security E1 From SA Operations Management and Security E2 From SA	1
Core Infrastructure Server Suite Standard (2 processor) System Center Standard (2 processor)	Operations Management and Security E1 From SA Operations Management and Security E2 From SA	2
Core Infrastructure Server Suite Datacenter (2 processor) System Center Datacenter (2 processor)	Operations Management and Security E1 From SA Operations Management and Security E2 From SA	8

¹Requires a minimum of four Qualifying Licenses

2.2 Microsoft Azure StorSimple Plan Offerings

For each StorSimple Plan with Device purchased, Customer will receive a Storage Array device. Geographic availability and the terms and conditions governing the Storage Array, including warranty, shipping and handling, and duties, are set forth in [Appendix F - Storage Array Terms](#). Each StorSimple Plan purchased by Customer will be associated with a single Storage Array; any additional Storage Arrays used by Customer will be billed at consumption rates.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Secure Productive Enterprise

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Secure Productive Enterprise E3 (User SL)						EO		
Secure Productive Enterprise E3 Add-on (User SL)						EO		
Secure Productive Enterprise E3 From SA (User SL)						EO		
Secure Productive Enterprise E5 (User SL)						EO		
Secure Productive Enterprise E5 Add-on (User SL)						EO		
Secure Productive Enterprise E5 From SA (User SL)						EO		
Skype for Business Plus CAL Add-on for Secure Productive Enterprise E3 (User SL)						A		

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All (except Secure Productive Enterprise From SA)	

2.1 Extended Use Rights for Secure Productive Enterprise Customers

2.1.1 Office Servers

Each Licensed User assigned a Secure Productive Enterprise User SL may:

- install any number of copies of the following server software on any Server dedicated to Customer's use: Exchange Server, SharePoint Server, and Skype for Business Server; and
- access to the above server software is exclusive to those users assigned a Secure Productive Enterprise User SL and External Users. This provision does not apply to customers who license Secure Productive Enterprise under the Microsoft Cloud Agreement.

2.1.2 Office Professional Plus

2.1.2.1 Secure Productive Enterprise From SA User SLs:

For each Licensed User to whom customer assigns a Secure Productive Enterprise From SA User SL, Customer may install:

- one local copy of Office Professional Plus for the sole use of the Licensed User for the duration of the subscription; and
- one local copy of Office Professional Plus for new User SLs added to the same volume license agreement for the sole use of the Licensed User for the duration of the subscription. The number of new User SLs granted those user rights may not exceed the number of From SA User SLs initially covered under the agreement.

This provision does not apply to customers who license this Product under the Microsoft Cloud Agreement.

2.1.2.1 Secure Productive Enterprise User SLs acquired in MPSA

For each Licensed User with a device covered with Software Assurance for Office Professional Plus to whom Customer assigns a Secure Productive Enterprise User SL, Customer may install one local copy of Office Professional Plus for the sole use of the Licensed User for the duration of the subscription.

2.2 Add-on User SLs and From SA User SLs

To acquire a Secure Productive Enterprise Add-On User SL or a Secure Productive Enterprise From SA User SL customer must satisfy the eligibility and [License](#) assignment requirements for each component of Secure Productive Enterprise. The components are: Windows 10 Enterprise E3/E5 Per User, Enterprise Mobility + Security E3/E5, and Office 365 Enterprise E3/E5. Refer to Secure Productive Enterprise Add-on User SLs and Secure Productive Enterprise From SA User SLs sub-sections in the Additional Information sections for the components of Secure Productive Enterprise for information.

2.3 From SA User SLs Purchases

Customer may not purchase more From SA User SLs than the number of Qualified Devices. As a one-time exception Customer may purchase a greater number of From SA User SLs, but only if (1) Customer purchases From SA User SL for each of the users of its Qualified Device, and (2) Customer must add devices as necessary to comply with the Primary use requirements in the Windows Desktop Operating System section 4.4.1.

2.4 SA Benefits for Secure Productive Enterprise From SA User SLs

Secure Productive Enterprise From SA User SLs provide the same SA Benefits as the From SA components of the Secure Productive Enterprise From SA User SL (Office 365 Enterprise E3/E5 From SA, Enterprise Mobility + Security From SA, and Windows 10 Enterprise E3/E5 Per User From SA).

2.5 United States Government Community Cloud Service

Refer to the Program Availability table for each component of Secure Productive Enterprise to find which components are [UC](#) services.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Enterprise Mobility + Security (Plan)

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Enterprise Mobility + Security E3 (User SL)	1	OM			P	EO	A	A,ST
Enterprise Mobility + Security E3 Add-on (User SL)	1	OM			P	EO	A	A,ST
Enterprise Mobility + Security E3 From SA (User SL)						EO		
Enterprise Mobility + Security E5 (User SL)	1	OM			P	EO	A	A,ST
Enterprise Mobility + Security E5 Add-on (User SL)	1	OM			P	EO	A	A,ST
Enterprise Mobility + Security E5 From SA (User SL)						EO		

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: Yes (Intune only)	True-Up Eligible: All	

2.1 Add-on User SL Purchase Eligibility

Customers must have an active Enterprise Enrollment with active SA for the corresponding Qualifying License(s). The Qualifying License(s) may be user-based or device-based. Customers with a pre-2010 version of the MBSA must sign the Online Services Supplemental Terms and Conditions.

2.2 Add-on User SL Qualifying Licenses

Qualifying License(s)	Add-on User SL
Core CAL Suite	Enterprise Mobility + Security
Enterprise CAL Suite	
Core CAL Suite Bridge for Office 365	
Core CAL Suite Bridge for Office 365 and Microsoft Intune	
Enterprise CAL Suite Bridge for Office 365	
Enterprise CAL Suite Bridge for Office 365 and Microsoft Intune	

2.3 Add-on User SL Purchase Restrictions

Only one Add-on User SL may be purchased for each Qualifying License (or set of Qualifying Licenses).

Customers may acquire Add-on User SLs for users or users of devices added to an Enterprise Enrollment user or device count between true-up dates (i.e., in advance of the acquisition of the qualifying licenses), subject to the same limitation of one Add-on User SL per Qualifying License (or set of Qualifying Licenses).

Campus and School Agreement customers may purchase the corresponding User Subscription License for Enterprise Mobility + Security User SLs for their Users up to the same quantity as their Eligible PC count so long as they have coverage for the Qualifying Licenses.

2.4 Purchase eligibility for Enterprise Mobility + Security From SA User SLs

From SA User SLs may be purchased in lieu of SA for fully paid, perpetual Licenses ("Qualifying Licenses") for the Products in the table below. From SA User SL may also be purchased instead of Subscription Licenses for the Products below if the Subscription License was purchased at least three years prior to the purchase of the From SA User SL. From SA User SLs requires CAL Suite Bridges as noted in the table.

Qualifying Licenses	Corresponding from SA User SL	Required CAL Suite Bridge
Core CAL Suite	Enterprise Mobility + Security from SA ¹	Core CAL Bridge for Enterprise Mobility + Security ^{2,3}
Enterprise CAL Suite	Enterprise Mobility + Security from SA ¹	Enterprise CAL Bridge for Enterprise Mobility + Security ^{2,4}

¹Available for purchase at enrollment anniversary or beginning of a new enrollment term only.

²Required for Purchase at enrollment anniversary only.

³Purchase not required for users also licensed with Office 365 (Enterprise & Government E1, E3, E5)

⁴Purchase not required for users also licensed with Office 365 (Enterprise & Government E3, E5)

2.5 From SA User SLs purchases

No more than one From SA User SL may be purchased for each per device Qualifying License in section 2.4. As a one-time exception for devices assigned a Qualifying License that are used by more than one user, Customer may purchase a From SA User SL for each of those users, but only if it purchases a From SA User SL for all users of all Qualified Devices.

2.6 SA Benefits for Enterprise Mobility + Security From SA User SLs

Enterprise Mobility + Security From SA User SLs qualify Customer for SA Benefits based on the Qualifying Licenses in section 2.4.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Dynamics 365 Services

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Dynamics 365 Plan 1, Enterprise edition (User SL)	1			A		A		A,ST
Microsoft Dynamics 365 Plan 2, Enterprise edition (User SL)	1			A		A		A,ST
Microsoft Dynamics 365 Plan 2 Enterprise edition Add-on (User SL)						A		A,ST
Microsoft Dynamics 365 Plan 2, Enterprise edition From SA (User SL)						A		A,ST
Microsoft Dynamics 365 for Customer Service, Enterprise edition (User SL)	1			A		A		A,ST
Microsoft Dynamics 365 for Customer Service, Enterprise Edition (Device SL)				A		A		A,ST
Microsoft Dynamics 365 for Field Service, Enterprise edition (User SL)	1			A		A		A,ST
Microsoft Dynamics 365 for Field Service, Enterprise edition (Device SL)				A		A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition (User SL)	1			A		A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition (Device SL)				A		A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition Add-on (Device and User SL)						A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition From SA (Device and User SL)						A		A,ST
Microsoft Dynamics 365 for Project Service Automation, Enterprise edition (User SL)	1			A		A		A,ST
Microsoft Dynamics 365 for Sales, Enterprise edition (User SL)	1			A		A		A,ST
Microsoft Dynamics 365 for Sales, Enterprise edition (Device SL)				A		A		A,ST
Microsoft Dynamics 365 for Team Members, Enterprise edition (User SL)	1			A		A		A,ST

Microsoft Dynamics 365 for Team Members, Enterprise edition Add-on (User SL)					A		A,ST
Microsoft Dynamics 365 for Team Members, Enterprise edition From SA (User SL)					A		A,ST
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Portal			A		A		A
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Portal Page Views			A		A		A
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Production Instance			A		A		A,ST
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Non-Production Instance			A		A		A,ST
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Database Storage			A		A		A
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Social Posts			A		A		A
Microsoft Dynamics 365 for Field Service, Enterprise edition - Resource Scheduling Optimization			A		A		A
Microsoft Dynamics 365 for Operations, Enterprise edition - Additional Database Storage			A		A		A
Microsoft Dynamics 365 for Operations, Enterprise edition - Additional File Storage			A		A		A
Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 1: Developer & Test Instance			A		A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 2: Standard Acceptance testing			A		A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 3: Premier Acceptance testing			A		A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 4: Standard Performance testing			A		A		A,ST
Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 5: Premier Performance testing			A		A		A,ST
Microsoft Dynamics 365 Enhanced Support			A		A		A,ST
Microsoft Dynamics 365 Pro Direct Support			A		A		A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: From SA User SLs, Add-on User SLs	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

2.1 Purchase Eligibility for Dynamics 365 From SA User SLs

From SA User SLs may be purchased instead of SA for fully paid, perpetual [Licenses](#) with active SA for the Qualifying Products in the table below. From SA User SLs may also be purchased instead of Subscription Licenses for the Products below if the Subscription License was purchased at least three years prior to the purchase of the From SA User SL. The From SA User SLs are only available for purchase at Enrollment anniversary or beginning of a new Enrollment term.

Qualifying Product(s)	Corresponding From SA User SL
Microsoft Dynamics AX Task CAL, Microsoft Dynamics AX Self Serve CAL, Microsoft Dynamics CRM Essentials CAL, or Microsoft Dynamics 365 for Team Members On-premises CAL	Microsoft Dynamics 365 for Team Members, Enterprise edition From SA
Microsoft Dynamics AX Task CAL (Device)	Microsoft Dynamics 365 for Operations, Enterprise Edition From SA (Device)
Microsoft Dynamics AX Functional CAL, or Microsoft Dynamics AX Enterprise CAL	Microsoft Dynamic 365 for Operations, Enterprise edition From SA Microsoft Dynamics 365, Enterprise edition Plan 2 From SA
Microsoft Dynamics CRM Basic CAL, or Microsoft Dynamics for Sales On-premises CAL	Microsoft Dynamics 365 for Sales, Enterprise edition From SA Microsoft Dynamics 365, Enterprise edition Plan 1 From SA
Microsoft Dynamics CRM Basic CAL, or Microsoft Dynamics 365 for Customer Service On-premises CAL	Microsoft Dynamics 365 for Customer Service, Enterprise edition From SA Microsoft Dynamics 365, Enterprise edition Plan 1 From SA
Microsoft Dynamics for Sales On-premises CAL	Microsoft Dynamics 365 for Case Management, Enterprise edition From SA
Microsoft Dynamics CRM Professional CAL	Microsoft Dynamics 365, Enterprise edition Plan 1 From SA

2.2 Add-on User SLs Qualifying Licenses

Each Qualifying License must have active SA. Only one Add-on User SL may be purchased for each Qualifying License (or set of Qualifying Licenses).

Qualifying License(s)	Add-on User SL
Microsoft Dynamics AX Task CAL, Microsoft Dynamics AX Self Serve CAL, or Microsoft Dynamics 365 Team Members CAL	Microsoft Dynamics 365 for Team Members, Enterprise edition Add-on
Microsoft Dynamics AX Task CAL (Device)	Microsoft Dynamics 365 for Operations, Enterprise edition Add-on (Device)
Microsoft Dynamics AX Functional CAL, or Microsoft Dynamics AX Enterprise CAL	Microsoft Dynamics 365 for Operations, Enterprise edition Add-on Microsoft Dynamics 365 Enterprise edition Plan 2 Add-on
Microsoft Dynamics CRM Basic CAL, or Microsoft Dynamics 365 for Sales On-premises CAL	Microsoft Dynamics 365 for Sales, Enterprise edition Add-on Microsoft Dynamics 365, Enterprise edition Plan 1 Add-on
Microsoft Dynamics CRM Basic CAL, or Microsoft Dynamics 365 for Customer Service On-premises CAL	Microsoft Dynamics 365 for Customer Service, Enterprise edition Add-on Microsoft Dynamics 365, Enterprise edition Plan 1 Add-on
Microsoft Dynamics 365 for Sales On-premises CAL	Microsoft Dynamics 365 for Case Management, Enterprise edition Add-on
Microsoft Dynamics CRM Professional CAL	Microsoft Dynamics 365, Enterprise edition Plan 1 Add-on

2.3 Unified Service Desk (USD)

Customers with active Microsoft Dynamics 365 Plan 1 or Plan 2, Enterprise edition subscriptions may install and use USD software for each user.

2.4 Microsoft Dynamics CustomerSource

Customers with active Microsoft Dynamics 365 Services subscriptions may access and use CustomerSource.

2.5 Eligibility for Qualified Offers

Customers renewing an agreement with Microsoft Dynamics CRM Online or Microsoft Dynamics AX Subscription Licenses as of November 1, 2016 or later may acquire Microsoft Dynamics 365 Online Services Qualified Offer in agreement renewals before October 31, 2019.

2.6 Microsoft Dynamics Marketing and Parature

Enterprise Agreement and Enterprise Agreement Subscription customers who have licensed Microsoft Dynamics Marketing and Parature, from Microsoft subscriptions prior to November 1, 2016 under a current Enrollment may renew their subscriptions in any subsequent Enrollment signed prior to July 1, 2017.

2.7 Microsoft Dynamics 365 Plan 2, Enterprise edition for Government

Microsoft Dynamics 365 for Operations is not available in Microsoft 365 Plan 2, Enterprise edition for Government.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office 365 Services

Office 365 Applications

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Office 365 Business		OM			OM, P		A	
Office 365 ProPlus (User SL)	2	OM			OM, P	E	A	EO,ST
Office 365 ProPlus From SA (User SL)						E		
Visio Pro for Office 365	1	OM			OM, P	A	A	A,ST
Visio Pro for Office 365 Add-on (User SL)						A		
Visio Pro for Office 365 From SA (User SL)						A		

2. Product Conditions

Terms of Service: OST	Product Pool: Applications	Extended Term Eligible: Visio Pro for Office 365
Migration Rights: N/A	Prerequisite: From SA User SL	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: Yes	True-Up Eligible: All	

2.1 Purchase Eligibility for Office 365 Applications From SA User SLs

From SA User SLs may be purchased instead of SA for fully paid, perpetual [Licenses](#) with active SA for the Qualifying Products in the table below. From SA User SL may also be purchased instead of Subscription Licenses for the Products below if the Subscription License was purchased at least three years prior to the purchase of the From SA User SL.

Qualifying Product(s)	Corresponding from SA User SL
Office Professional Plus	Office 365 ProPlus From SA
Visio Professional	Visio Pro for Office 365 From SA

2.2 Add-on User SLs Qualifying Licenses

Each Qualifying License must have active SA.

Qualifying Product(s)	Add-on User SL
Visio Professional	Visio Pro for Office 365 Add-on to Visio Professional
Visio Standard	Visio Pro for Office 365 Add-on to Visio Standard

2.3 Media Eligibility for Office 365 Pro Plus with Windows To Go Rights

If a user to whom Customer has assigned an Office 365 ProPlus License uses software under Windows to Go Rights, then in lieu of installing a copy of the software provided with Office 365 ProPlus on one of the five permitted devices pursuant to the terms of service for Office 365 ProPlus, that user may 1) install one copy of the Office Professional Plus 2013 software on the USB drive used for Windows to Go Rights, and 2) use the Office Professional Plus 2013 software on that USB drive on any device. Upon termination of Customer's Office 365 ProPlus subscription it must uninstall Office Professional Plus 2013 software from the USB drive.

2.4 Campus and School Agreement, Enrollment for Education Solutions and Open Value Subscriptions – Education Solutions

If Customer is an Institution as described in the Campus and School Agreement and subscribes to Office 365 ProPlus User SL, it must purchase a License for each Qualified User in the Institution's organization. If Institution signs up for Student Option for Office 365 ProPlus User SL, it must purchase a [License](#) for each Student in the Organization.

Institutions with Office 365 ProPlus User SLs assigned to all faculty and staff may install Office Professional Plus 2016 software on any open access lab or library within the Institution's Organization. Use of the software is otherwise subject to the License terms for Office Professional Plus 2016.

Institutions with Office Professional Plus Software Assurance assigned to all faculty and staff are eligible to acquire Licenses for Office 365 ProPlus for all faculty and staff part of Institution's organization at no additional cost to Institution. Licenses acquired at no cost through this offer may not be counted toward satisfaction of Institution's minimum order requirements.

2.5 Office Multi Language Pack

Customers with Office 365 Application subscriptions may use the latest version of the Office Multi Language Pack with copies of desktop applications software they are permitted to use under their qualifying Office 365 subscription. The right to use the Office Multi Language Pack expires upon the expiration of rights under the qualifying Office 365 Application.

2.6 E-Learning

Customer may access hosted E-Learning courses if it has one or more Licenses for Office 365 ProPlus (SCORM-compliant content is not eligible). Only Customer's users with active Office 365 ProPlus licenses may access hosted online E-Learning courses relevant to Office 365 ProPlus services by logging in to the Online Training site with their Office 365 ProPlus credentials. Customer's use of hosted E-Learning courses is subject to the E-Learning website terms of use.

2.7 Office Online

If Customer has a [License](#) for Office 365 ProPlus, then Customer may use Office Online services. Each of Customer's [Licensed Users](#) of Office 365 ProPlus may access Office Online services for viewing and editing documents, as long as they are also licensed for SharePoint Online or OneDrive for Business.

2.8 Open Value Subscription Migration Period

For each unit of Office 365 ProPlus, Midsize Business, Enterprise E3-E5, or Education E3-E5 User SLs Customer activates on or before the expiration of their Open Value Subscription agreement (the "Expiration Date"), Customer may continue to use the copy of Office Standard or Professional Plus licensed to them under an Open Value Subscription agreement. This right expires 180 days after the Expiration Date. Use of Office Standard or Office Professional Plus during this period is subject to the Use Rights effective on the Expiration Date.

2.9 Deployment Rights for Visio Professional 2016

Each Office 2016 users with a subscription for Visio Pro for Office 365 may install and use a single copy of Visio Professional 2016 software on the device on which Office 2016 is installed.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office 365 Suites

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Office 365 Business Essentials		OM			OM, P		A	
Office 365 Business Premium		OM			OM, P		A	
Office 365 Education (User SL)	1						A	AO,ST
Office 365 Education E5 (User SL)	(1)						A	EO,ST
Office 365 Education E5 Add-on (User SL)	(1)						A	EO,ST
Office 365 Enterprise E1 (User SL)	1	OM		UC	EO,OM, P	EO,UC		
Office 365 Enterprise E1 From SA (User SL)						EO,UC		
Office 365 Enterprise E3 (User SL)	1	OM		UC	EO,OM, P	EO,UC		
Office 365 Enterprise E3 From SA (User SL)						EO,UC		
Office 365 Enterprise E4 (User SL)	1			UC				
Office 365 Enterprise E4 From SA (User SL)						UC		
Office 365 Enterprise E5 (User SL)	1	OM			EO,OM, P	EO		
Office 365 Enterprise E5 From SA (User SL)						EO		
Office 365 Enterprise E1, E3 Add-on (User SL)	1			UC	OW	EO,UC		
Office 365 Enterprise E4 Add-on (User SL)	1			UC		UC		
Office 365 Enterprise E5 Add-on (User SL)					OW	EO		
Office 365 Enterprise E3 without ProPlus Add-on (User SL)						EO,UC		
Office 365 Enterprise E4 without ProPlus Add-on (User SL)						UC		
Office 365 Enterprise K1 (User SL)	1			UC		A,UC		
Office 365 Midsize Business (User SL)		OM			P			

2. Product Conditions

Terms of Service: OST	Product Pool: All Application and Server (E1 and K1 Server only), MPSA – All Application only	Extended Term Eligible: Enterprise, Government, K
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: K only	Reduction Eligible: Enterprise, Government, K	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: Enterprise, Government, K	

2.1 United States Government Community Cloud Service

For Office 365 Suites identified above in Program Availability as **UC**, refer to the program availability table for each suite component to find which components are **UC** services.

2.2 Campus and School Acquisitions

Under Campus and School Agreement, subscription licenses for Office 365 Suites must be acquired per user on an Institution-wide or non-Institution-wide basis. If additional User SLs are required to access Office 365 Suites mid-term, Institution must submit an order for such [Licenses](#). When licensing Office 365 Add-on, the corresponding qualifying License must be licensed under the same Enrollment. When placing anniversary orders, Institution may order fewer [Licenses](#) for Online Services than the quantity of Institution's initial order as long as the anniversary order meets the minimum requirements for Platform Online Services as set forth in Customer's volume licensing agreement.

2.3 No cost Office 365 ProPlus Student Licensing Based on Faculty/Staff Coverage

Provided an Institution has licensed Office Professional Plus or Office 365 ProPlus for all Faculty and Staff in its defined Organization under an Open Value Subscription Agreement for Education Solutions or a Campus and School Agreement Enrollment for Education Solutions, Institution is eligible to acquire Licenses for Office 365 ProPlus for all students enrolled in any educational institution that is part of Institution's defined Organization, whether on a full-time or part-time basis, at no additional cost to Institution. [Licenses](#) acquired at no cost through this offer may not be counted toward satisfaction of Institution's minimum order requirements.

2.4 Campus and School Lab or Library Use

Refer [Office 365 ProPlus Product Entry](#) for offer to use Office Professional Plus 2016 software on any open access lab or library within the Institution's Organization for Institutions with Office 365 ProPlus User SLs assigned to all faculty and staff.

2.5 Add-on User SLs Qualifying Licenses

Qualifying License(s)	Add-on User SL
Core CAL Suite ¹	- Office 365 Enterprise E1 Add-on² - Office 365 Enterprise E1 w/Exchange Online Archiving Add-on^{2,3,4} - Office 365 Government E1 Add-on

	- Office 365 Enterprise & Government E3 without ProPlus Add-ons - Office 365 Government E4 without ProPlus Add-ons - Office 365 Education E5 Add-on - Exchange Online Plan 1 Add-on - Skype for Business Online Plan 1 Add-on - SharePoint Online Plan 1 Add-on
Core CAL Suite ¹ + Office Professional Plus ¹	- Office 365 Enterprise E1 / Government E1 Add-ons - Office 365 Enterprise E3 Add-on² - Office 365 Government E3 Add-on⁴ - Office 365 Enterprise & Government E4, E5 Add-ons - Office 365 Enterprise & Government E3 without ProPlus Add-ons - Office 365 Government E4 without ProPlus Add-ons - Office 365 Education E5 Add-on - Office 365 Midsize Business Add-on² - Exchange Online Plan 1 Add-on - Skype for Business Online Plan 1 Add-on - SharePoint Online Plan 1 Add-on
Enterprise CAL Suite ¹	- Office 365 Enterprise & Government E3 without ProPlus Add-ons - Office 365 Enterprise & Government E4⁴ without ProPlus Add-ons - Office 365 Education E5 Add-on - Azure Information Protection Premium Add-on
Enterprise CAL Suite ¹ + Office Professional Plus ¹	- Office 365 Enterprise & Government E3², E4², or E5 Add-ons - Office 365 Education E5 Add-on - Office 365 Enterprise & Government E3² or E4⁴ without ProPlus Add-ons
Office Professional Plus ¹	- Office 365 Midsize Business Add-on^{2,3} - Office 365 Enterprise E3 Add-on^{2,3} - Office 365 Education E5 Add-on

¹Each Qualifying License must have active SA

²These are the only offerings available to Open Value and Open Value Subscription customers.

³This Add-on User SL may only be purchased under an Open Value (Organization Wide) or Open Value Subscription agreement.

⁴Only Government customers as defined in Customer's volume licensing agreement may purchase this Add-on User SL.

Add-on User SLs (other than the Office 365 Midsize Business Add-on) have access rights equivalent to the Qualifying License, and permit the licensed user to access the same functionality of Customer's corresponding on-premises server Products as the Qualifying License from any device.

2.6 Purchase Restrictions

Only one Add-on User SL may be purchased for each Qualifying License (or set of Qualifying Licenses).

Customers may acquire Add-on User SLs for users or devices added to an Enterprise Enrollment user or device count, or to an Open Value Subscription Agreement, between true-up dates (i.e., in advance of the acquisition of the Qualifying Licenses), subject to the same limitation of one Add-on User SL per qualifying License (or set of Qualifying Licenses).

2.7 Volume Licensing Program Terms

Programs terms applicable to the corresponding Online Service User SL also apply to the Add-on User SLs.

2.8 Purchase eligibility for Office 365 From SA User SLs

From SA User SLs may be purchased instead of SA for fully paid, perpetual Licenses with active SA for the Qualifying Products in the table below. From SA User SL may also be purchased instead of Subscription Licenses for the Qualifying Products below if the Subscription License was purchased at least three years prior to the purchase of the From SA User SL.

Qualifying Products	Corresponding from SA User SL	Required CAL Suite Bridge
Core CAL Suite	Office 365 (Enterprise E1 & Government E1) From SA ¹	Core CAL Bridge for Office 365 ^{2,3}
Office Professional Plus and Core CAL Suite	Office 365 (Enterprise E3, E5 & Government E3, E4) From SA ¹	Core CAL Bridge for Office 365 ^{2,3}
Office Professional Plus and Enterprise CAL Suite	Office 365 (Enterprise E3, E5 & Government E3, E4) From SA ¹	Enterprise CAL Bridge for Office 365 ^{2,3}

¹Available for purchase at enrollment anniversary or beginning of a new enrollment term only.

²Required for Purchase at enrollment anniversary only.

³Purchase not required for users also licensed with Enterprise Mobility + Security.

At their next Enrollment renewal, customers who have licensed Office 365 suite subscriptions prior to August 1, 2014 under a current Enrollment may purchase corresponding From SA User SLs to license all respective Office 365 users including those users added during the remainder of their current Enrollment term.

2.9 From SA User SLs purchases

No more than one From SA User SL may be purchased for each per device Qualifying License in section 2.8. As a one-time exception for devices assigned Qualifying Licenses that are used by more than one user, Customer may purchase a From SA User SL for each of those users, but only if it purchases a From SA User SL for all users of all licensed Qualified Device.

2.10 SA Benefits for Office 365 From SA User SLs

Office 365 (Enterprise E1, E3, E5 and Government E1, E3, E4) From SA User SLs provide the same SA Benefits as the Qualifying Products in section 2.8 above.

2.11 Office 365 Enterprise K1

Office 365 Enterprise K1 is formerly known as Business Productivity Online Deskless Suite (BPOS Deskless). Customers in Brazil and Chile purchasing Office 365 Enterprise K1 will be provisioned on BPOS Deskless. These customers may migrate to Office 365 Enterprise K1.

2.12 Office Multi Language Pack

Customers with Office 365 Suite that include Office 365 ProPlus may use the latest version of the Office Multi Language Pack with copies of desktop applications software they are permitted to use under their qualifying Office 365 Suite.

2.13 E-Learning

Customer may access hosted E-Learning courses if it has one or more Licenses for Office 365 ProPlus (SCORM-compliant content is not eligible). Only Customer's users with active Office 365 ProPlus licenses may access hosted online E-Learning courses relevant to Office 365 ProPlus services by logging in to the Online Training site with their Office 365 ProPlus credentials. Customer's use of hosted E-Learning courses is subject to the E-Learning website terms of use.

2.14 Office 365 Midsize Business Product Key Redemption

Office 365 Midsize Business is available until September 30, 2015, after which unredeemed subscriptions may be used for a successor product.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office 365 Advanced Security Management

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Office 365 Advanced Security Management (User SL)	1	OM			P	A	A	A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: All	Reduction Eligible: All	Reduction Eligible (SCE): All
Student Use Benefit: All	True-Up Eligible: All	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office 365 Customer Lockbox

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Office 365 Customer Lockbox (User SL)		OM		UC	P	A,UC	A	A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: N/A
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: All	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft MyAnalytics

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft MyAnalytics (User SL)		OM			P	A	A	A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: N/A
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: All	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Office 365 Advanced Compliance

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Office 365 Advanced Compliance (User SL)		OM			P	A	A	A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: N/A
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: All	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Exchange Online

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Exchange Online Plan 1 (User SL)		OM		UC	OM, P	A,UC		A
Exchange Online Plan 1 Add-on (User SL)		OM		UC	P	A,UC	A	
Exchange Online Plan 1A for Alumni (User SL)								A
Exchange Online Plan 2 (User SL)	1	OM		UC	P	A,UC	A	A,ST
Exchange Online Kiosk (User SL)				UC		A,UC		
Exchange Online Archiving for Exchange Online (User SL)	1	OM		UC	P	A,UC	A	A,ST
Exchange Online Archiving for Exchange Server (User SL)	1	OM		UC	P	A,UC	A	A,ST
Exchange Online Protection (User SL)		OM		UC	OM, P	A,UC	A	A
Office 365 Advanced Threat Protection (User SL)		OM		UC	P	A,UC	A	A,ST
Import Service for Office 365						A		

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All (except Encryption)
Migration Rights: Product List - March 2014 (Exchange Hosted Archive)	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: K only	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

2.1 Exchange Online Archiving for Exchange Server

Exchange Online Archiving for Exchange Server is a successor Online Service to Exchange Hosted Archive.

2.2 Exchange Online Archiving for Exchange Server A

Academic Institutions under Enrollment for Education Solutions and Open Value Subscription Agreement for Education Solutions, licensed for Enterprise CAL Suite for their Organization-Wide count and Student count are authorized to a corresponding number of Exchange Online Archiving for Exchange Server A User SLs for all users covered within their Organization-Wide count and Student count.

2.3 Prerequisite: Add-on User SLs

Refer to Add-on User SLs in [Office 365 Suites](#) for information on Add-ons.

[Table of Contents](#) / [Glossary](#) / [Index](#)

OneDrive for Business

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
OneDrive for Business Plan 1 (User SL)	1	OM		UC	P	A,UC	A	
OneDrive for Business Plan 2 (User SL)	1	OM		UC	P	A,UC	A	

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Project Online

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Project Online Essentials (User SL)	1	OM			P	A,UC		
Project Online Essentials Add-on (User SL)						A,UC		
Project Online Professional (User SL)	1	OM			OM, P	A,UC	A	A,ST
Project Online Professional Add-on (User SL)						A,UC		
Project Online Professional From SA (User SL)						A,UC		
Project Online Premium (User SL)	1	OM			OM, P	A,UC	A	A,ST
Project Online Premium Add-on (User SL)						A,UC		
Project Online Premium From SA (User SL)						UC		

2. Product Conditions

Terms of Service: OST	Product Pool: Server, MPSA - All Application only	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

2.1 Purchase Eligibility for Project Online From SA User SLs

From SA User SLs may be purchased instead of SA for fully paid, perpetual [Licenses](#) with active SA for the Qualifying Products in the table below. From SA User SL may also be purchased instead of Subscription Licenses for the Products below if the Subscription License was purchased at least three years prior to the purchase of the From SA User SL. The from SA User SLs are only available for purchase at enrollment anniversary or beginning of a new enrollment term.

Qualifying Products	Corresponding from SA User SL
Project Professional	Project Online Professional From SA Project Online Premium From SA
Project Server CAL	Project Online Professional From SA Project Online Premium From SA

2.2 Add-on User SLs Qualifying Licenses

Each Qualifying License must have active SA.

Qualifying License(s)	Add-on User SL
Project Professional	Project Online Professional Add-on to Project Professional Project Online Premium Add-on to Project Professional
Project Standard	Project Online Professional Add-on to Project Standard Project Online Premium Add-on to Project Standard
Project Server CAL	Project Online Essentials Add-on to Project CAL Project Online Professional Add-on to Project CAL Project Online Premium Add-on to Project CAL

2.3 Office Multi Language Pack

Customers with Project Online Professional or Project Online Premium subscriptions may use the latest version of the Office Multi Language Pack with copies of desktop applications software they are permitted to use under their qualifying subscription. The right to use the Office Multi Language Pack expires upon the expiration of rights under the qualifying subscription.

2.4 Deployment Rights for Project Professional 2016

Each Office 2016 users with a subscription for Project Online Professional or Project Online Premium may install and use a single copy of Project Professional 2016 software on the device on which Office 2016 is installed.

2.5 Project Online and Project Pro for Office 365 Product Key Redemption

Project Online and Project Pro for Office 365 subscriptions licensed through Open, Open Value, or Open Value Subscription agreements may be redeemed until December 31st, 2016, after which unredeemed subscriptions may be used for a successor product.

[Table of Contents](#) / [Glossary](#) / [Index](#)

SharePoint Online

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
SharePoint Online Plan 1 (User SL)	1	OM		UC	P	A,UC		
SharePoint Online Plan 1 Add-on (User SL)						A		
SharePoint Online Plan 2 (User SL)	1	OM		UC	P	A,UC		
Office 365 Extra File Storage 1 GB (Add-on SL)	1	OM		UC	P	A,UC	A	A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: K only	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All	

2.1 Prerequisite: Add-on User SLs

Refer to Add-on User SLs in [Office 365 Suites](#) for information on Add-ons.

2.2 SharePoint Online Plan 1 with Yammer and SharePoint Online Plan 2 with Yammer Key Redemption

SharePoint Online Plan 1 with Yammer or SharePoint Online Plan 2 with Yammer subscriptions licensed through Open, Open Value, or Open Value Subscription agreements may be redeemed until October 31, 2015, after which unredeemed subscriptions may be used for a product that includes either of those services.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Skype for Business Online

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Skype for Business Online Plan 1 (User SL)	1	OM		UC	OM, P	A,UC		
Skype for Business Online Plan 1 Add-on (User SL)						A,UC		

Skype for Business Online Plan 2 (User SL)	1	OM		UC	OM, P	A,UC		
Skype for Business Online Cloud PBX (User SL)		OM			P	A		A,ST
Skype for Business Online PSTN Conferencing (User SL)		OM			P	A,UC	A	A,ST
Skype for Business Online PSTN Calling (User SL)						A		A,ST
Skype for Business PSTN Consumption (User SL)						A		

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All (except for Skype for Business PSTN Consumption)	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: All (except for Skype for Business PSTN Consumption)	

2.1 Lync for Mac 2011

Skype for Business Online Plan 1 and Plan 2 require the separate purchase and installation of Skype for Business 2015 (or Lync for Mac 2011) to access the complete feature set of Skype for Business Online Plan 1 and Plan 2. As a limited time offer, customers licensed for Skype for Business Online receive one licensed copy of Lync for Mac 2011 at no cost with each trial or paid subscription [License](#) to Skype for Business Online. The software may only be used with Skype for Business Online, and all rights to use the software will terminate upon expiration of the underlying subscription [License](#) or migration to the next version of Skype for Business Online, whichever comes first. Customers may use the free Skype for Business Basic 2015 client for their Windows-Based end users.

2.2 Prerequisite: Add-on User SLs

Refer to Add-on User SLs in [Office 365 Suites](#) for information on Add-ons.

2.3 Skype for Business PSTN Consumption

Skype for Business PSTN Consumption services require an initial payment through the Office 365 Administration Portal. Microsoft will invoice Customer or its reseller immediately for each transaction including, if automatic replenishment is enabled, each time the minimum balance is reached. Any funds customer allocates to the Skype for Business PSTN Consumption services may be used for those services, and any such funds not used within 12 months from the date of the transaction will be forfeited.

Usage charges will be based on Microsoft's published rates when the services are used. Skype for Business PSTN Consumption services are exempt from fixed pricing, notwithstanding any reference to fixed pricing under the applicable volume licensing agreement.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Other Online Services

Bing Maps

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Bing Maps Enterprise Fee Monthly Subscription	25				P	A		
Bing Maps Asset Management Platform Monthly Subscription	25				P	A		
Bing Maps Internal Website Usage 100K Transactions Monthly Subscription	125				P	A		
Bing Maps Internal Website Usage 500K (and higher) Transactions Monthly Subscription	200				P	A		
Bing Maps Known Per User Monthly Subscription	1				P	A		
Bing Maps Known 5K User Monthly Subscription	200				P	A		
Bing Maps Light Known 500 User Monthly Subscription	1				P	A		
Bing Maps Light Known 5K User Monthly Subscription	125				P	A		
Bing Maps Asset Management for Windows	1				P	A		
Bing Maps Public Website Usage 100K Transaction Monthly Subscription	50				P	A		
Bing Maps Public Website Usage 500K (and higher) Transactions Monthly Subscription	200				P	A		

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: N/A
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: N/A	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: N/A	

2.1 Billable Transactions

Each Bing Maps Public Website Usage Add-on SL and Bing Maps Internal Website Usage Add-on SL entitles the Customer to the number of Billable Transactions specified in the Product name. On either the enrollment or subscription expiration date, all purchased and unused Billable Transactions are forfeited.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Business Application Platform

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Flow Plan 1 (User SL)				A		A		A,ST
Microsoft Flow Plan 2 (User SL)				A		A		A,ST
Microsoft PowerApp Plan 1 (Device and User SL)				A		A		A
Microsoft PowerApp Plan 2 (User SL)				A		A		A,ST
Power BI Pro	1	OM		UC	OM, P	A,UC		
Power BI Pro A	1	OM					A	A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: Flow and PowerApp
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: Power BI Pro	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: Flow and PowerApp	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Intune

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Intune (User SL)	1	OM			P	EO, A	A	A,ST
Microsoft Intune Add-on (User SL)	1	OM			P	A	A	A,ST
Microsoft Intune User SL Add-on Extra Storage 1 GB	1					A		A,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: All
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: Yes	True-Up Eligible: All	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Learning

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Learning E-Reference Library	1					A	A	A

Attachment E - Page 117 of 245

[Table of Contents](#)

[Introduction](#)

[License Terms](#)

[Software](#)

[Online Services](#)

[Glossary](#)

[Appendices](#)

[Index](#)

Microsoft Learning Imagine Academy	75	OM					A	A
Microsoft Learning MCP 1 Exam Vouchers (Services SL)	1					A	A	A
Microsoft Learning MCP 30 Exam Vouchers (User SL)	75	OM					A	A
Microsoft Learning MTA/MCA Certification 125 Exam Site License (Services SL)	125						A	A
Microsoft Learning MOS/MCE Certification 125 Exam Site License (Services SL)	125						A	A
Microsoft Learning MOS/MTA/MCE Certification 500 Exam Site License (Services SL)	125						A	A

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: N/A
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: N/A	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: N/A	

2.1 Vouchers

Vouchers are provided upon purchase and expire 12 months from date of purchase.

2.2 Microsoft Office Specialist (MOS) Microsoft Technology Associate (MTA) and Microsoft Certification Educator (MCE) Exam Site License

Customer must be a Certiport/Pearson VUE test center authorized to deliver MOS or MTA exams under a site [License](#). The site [License](#) will expire 12 months from the date of purchase. Any undelivered exams at the end of the term are forfeited. Academic Customers may only deliver site license exams to their faculty members and registered students.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Microsoft Translator

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Microsoft Translator API						A		

2. Product Conditions

Terms of Service: OST	Product Pool: Server	Extended Term Eligible: N/A
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: All	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: N/A	

[Table of Contents](#) / [Glossary](#) / [Index](#)

Minecraft: Education Edition

1. Program Availability

Online Services	Point	OL	S/S+	MPSA	OV/OVS	EA/EAS	OVS-ES	EES
Minecraft: Education Edition	1							AO,ST

2. Product Conditions

Terms of Service: OST	Product Pool: Application	Extended Term Eligible: N/A
Migration Rights: N/A	Prerequisite: N/A	Promotions: N/A
Qualified User Exemption: N/A	Reduction Eligible: N/A	Reduction Eligible (SCE): N/A
Student Use Benefit: N/A	True-Up Eligible: N/A	

2.1 Eligibility for No Charge Student Offering

Institutions may acquire Licenses of Minecraft: Education Edition at no charge for its students if it has purchased Licenses of the Minecraft: Education Edition Faculty offering for all of its Faculty and Staff. Licenses acquired by this method are not eligible for fulfilling any order requirements.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Glossary

Attributes

Attributes are identified in the tables in each Product Entry, and indicate rights or conditions applicable to the Products.

Additional Software: Software identified in the Use Rights for Server Products that Customer is permitted to use on any device in conjunction with its use of server software.

Client Access Requirement: Indicates whether or not a Server Product requires CALs for access by users and devices.

Disaster Recovery: Rights available to SA customers to use software for conditional disaster recovery purposes; refer to [Servers – Disaster Recovery Rights](#) section of [Appendix B – Software Assurance](#) for details.

Down Editions: Permitted lower editions corresponding to specified higher editions. Customer may use the permitted lower edition in place of a licensed higher-level edition, as permitted in the Universal License Terms.

Extended Term Eligible: Online services that are eligible for an extended term as described in the Enterprise and Enterprise Subscription licensing agreement.

External User Access Requirement: Indicates specific license requirements or options for access by [External Users](#).

Fail-Over Rights: An SA benefit that allows Customer to run passive fail-over Instances of the Product in conjunction with software running on the [Licensed Server](#), in anticipation of a fail-over event. Passive fail-over Instances may be run in either a separate [OSE](#) on the [Licensed Server](#) or on a different [Server](#) dedicated to Customer's use. Fail-Over Rights apply only if the number of licenses that otherwise would be required to run the passive fail-over Instances does not exceed the number of licenses required to run the corresponding production Instances.

Government Community Cloud (U.S. only): Online Services that are available exclusively to qualifying United States federal, state, local, or tribal government entities. Use Rights for government community cloud services are equivalent to those of their standard multi-tenant equivalents unless otherwise noted. Qualifying Online Services are offered as government community cloud services and non-government community cloud services. Customers may be provisioned as one or the other but not a mix of both. Online Services designated as government community cloud may not be deployed in the same domain with specific non-government community cloud services.

Included Technologies: Indicates other Microsoft components included in a Product; refer to the Included Technologies section of Universal License Terms for details.

License Mobility: Rights available to SA customers either to reassign licenses outside the standard timelines or to use Products on multi-tenant servers outside their own datacenters; refer to License Mobility section of [Appendix B – Software Assurance](#) for details.

License Terms: Terms and conditions governing deployment and use of a Product.

Migration Rights: Customer may be able to upgrade from prior versions of the software or other Products under special terms published in the Product Entry or Product List as indicated. Customer may also have non-standard downgrade rights to use prior versions of the same or other Products in place of the licensed version.

Prerequisite: Indicates that certain additional conditions must be met in order to purchase Licenses for the Product.

Prerequisite (SA): Indicates that certain additional conditions must be met in order to purchase SA coverage for the Product.

Prior Version: Earlier versions of Product and their Date Available.

Notices: Identifies the notices applicable for a Product; refer to the Notices section of the [Universal License Terms](#) for details.

Online Subscription Program (OSP): The Product is available in an Online Subscription program.

Product Pool: Indicates the grouping of Products that the Product belongs to for the purposes of determining pricing discounts. There are three Product pool categories; Application, Server and System.

Product-Specific License Terms: Indicates that Product-Specific terms and conditions governing deployment and use of the Product are included below the Use Rights table.

Promotions: Indicates that limited time offers apply to the Product as described in [Appendix E – Promotions](#).

Qualified User Exemption: Exemption applicable to users who access Products solely under one of these licenses. These users are exempt from being counted as a Qualified User under Customer's volume licensing agreement, notwithstanding anything to the contrary in that agreement.

Reduction Eligible: An Online Service for a customer that has an Enterprise Enrollment, Enterprise Subscription Enrollment, Microsoft Azure Enrollment or Enrollment for Education Solutions can report a reduction in licenses or Allocated Annual Commitment.

Reduction Eligible (SCE): Products for which a Server & Cloud Enrollment customer can report a reduction in subscription licenses or future Allocated Annual Commitment after 12 continuous months.

Roaming Rights: An SA benefit that permits the [Primary User](#) of a [Licensed Device](#) certain access and use rights. The [Primary User](#) may use a [Qualifying Third Party Device](#) to (i) remotely access and use permitted Instances or copies of the software running on [Servers](#) dedicated to Customer's use, (ii) locally use a permitted Instance or copy in a [Virtual OSE](#), or (iii) locally access a permitted Instance or copy of the software on a USB drive via Windows to Go, in each case solely for work-related purposes while the user is not on Customer's premises. No other user may use the software under the same [License](#) at the same time. Despite anything to the contrary in Customer's volume licensing agreement, Qualified Desktops and Devices do not include any Qualifying Third Party Devices from which Customer's users access and use the software and any (other) enterprise product solely under Roaming Rights.

SA Equivalent Rights: Software [SLs](#) acquired under a Server and Cloud Enrollment or Microsoft Products and Services Agreement provide the same SA rights and benefits during the term of the Subscription as [Licenses](#) with SA coverage.

Self Hosting: An SA benefit that permits use of Products for conditional hosting purposes; refer to the Servers – Self Hosted Applications section of [Appendix B – Software Assurance](#) for details.

SA Benefits Pool: Indicates the category of the Product for purposes of determining SA Benefits broadly applicable to that Product Pool, as listed in [Appendix B – Software Assurance](#).

Student Use Benefit: The option for Institutions that license a qualifying Product for their Organization-wide Count to license a Product for use by their Students at no additional cost. The qualifying Product and the Product eligible for the Student Use Benefit are identified in the Product Entry. Such Student Licenses may not be counted toward minimum order requirements.

Suite: A Product that is comprised of components that are also licensed separately. A suite is licensed under a single [License](#) that is assigned to a single user or device, and allows use of all of its components on the single device or by a single user to which it is assigned. The components of the Suite may not be separated and used on separate devices or by separate users.

True-Up Eligible: An Online Service subscription License that an Enterprise or Enterprise Subscription customer can order via the true-up or annual order process rather than monthly.

UTD Discount: An Up to Date Discount is a discount available to Open Value Subscription customers ordering licenses for Product during the first year of their agreement if they have a [License](#) for the corresponding qualifying Product.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Cell Values

Cell Values are used in the Program Availability table in each of each Product Entry to identify how the Product is offered in each program. The volume licensing program agreements define these offering types.

A= Additional Product: The Product is offered as an Additional Product.

AO= Additional Product Organization Wide: The Product is offered as an Additional Product orderable organization-wide.

E = Enterprise Product: The Product is offered as an Enterprise Product, but not a desktop.

ED = Education Desktop: The Product is offered as an education desktop platform product with either Enterprise CAL Suite or Core CAL Suite under Enrollment for Education Solutions and Open Value Subscription – Education Solutions.

EO = Enterprise Online Service: The Online Service is offered as an enterprise Online Service or platform Online Service and satisfies the Enterprise Product requirements. EO for Core CAL and Enterprise CAL Suite require the corresponding CAL Suite Bridge.

OM = Open Minimum: Each License counts solely as 5 Licenses for purposes of the initial order minimum in Open License and Open Value.

OW = Organization-wide: Available under the Organization-wide option.

P = Non-Organization Wide in Open Value: The Product is offered on a non-Organization Wide basis in Open Value.

SD= School Desktop Platform Product: The Product is offered as a school desktop platform product with either Enterprise CAL Suite or Core CAL Suite under Campus and School Agreement. An SD is counted as three units.

ST = Student Offering: The Product is offered as a Student Offering and must be ordered for the full Student Count.

SP = Server and Tools Product: The Product is a server and tools product offered under the Server and Cloud Enrollment.

UC = United States Government Community Cloud Service: The Online Service is offered as a United States Government Community Cloud Service.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Column Headings

Column Headings appear in the Program Availability table for each Product Entry and organize program availability information by program, offering type, points and availability dates.

DA= Date Available: The date a Product is first available, designated as month/year. For software, it is the earlier of the date Microsoft makes licenses available for ordering or available for download from the Volume Licensing Services Center (VLSC).

EA/EAS = Enterprise Agreement and Enterprise Subscription Agreement: Includes Enterprise and Enterprise Subscription Enrollments, including the Server Cloud Enrollment.

EES = Enrollment for Education Solutions: Includes Enrollment for Education Solutions and the School Enrollment under the Campus and School Agreement (CASA).

L = License: Point value designated for the software License indicated. If point value is parenthesis, that is the value for CASA.

L/SA = License and SA: Point value designated when License and SA is offered for purchase at the same time.

MPSA = Microsoft Products and Services Agreement.

OL = Open License: Open License includes Open License, Open License for Academic, Open License for Government, and Open License for Charity, where available.

OV/OVS= Open Value and Open Value Subscription: Includes Open Value, Open Value Subscription, Open Value for Government, and Open Value Subscription for Government.

OVS-ES= Open Value Subscription – Education Solutions.

Point = The value assigned to a Product used to calculate the volume pricing level applicable to Customer's volume licensing agreement.

SA = Software Assurance: Point value designated when SA is offered for the software indicated.

S/S+ = Select and Select Plus: This also includes Select for Academic, Select Plus for Academic, Select for Government, and Select Plus for Government.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Definitions

Academic Program means Academic Purchasing Account on MPSA, Academic Select License, Select Plus for Academic, Campus and School Agreement, or Open Value Subscription – Education Solutions.

Add-on means a license that is purchased in addition to (and associated with) a previously acquired Qualifying License (or set of Qualifying Licenses) and is assigned to a single Qualified User (as defined in Customer's Enrollment). For any Add-on User SL not appearing individually in OST, the license terms applicable to a full User SL for the same service apply.

Additive CAL means a [CAL](#) that must be used on conjunction with a base [CAL](#).

Additive External Connector License means an [External Connector License](#) that must be used in conjunction with a base [External Connector License](#).

CAL means client access license, which may be assigned by user or device, as appropriate. A user CAL allows access to corresponding version of the server software or earlier versions of the server software from any device by one user. A device CAL allows access to corresponding versions of the server software or earlier versions of the server software from one device by any user. CALs allow access to server software running on Customer's Licensed Servers only.

CAL Equivalent License means a User [SL](#) or [External Connector License](#) identified in a Product's "Server Software Access" table, or a [CAL](#) suite or [SL](#), as identified in the CAL Equivalent Licenses Table, [Appendix A](#), as applicable. A CAL suite is a CAL Equivalent License only if Customer purchased the [License](#) after the Server Product's Date Available or if Customer had active SA coverage as of the Date Available.

Client OSE means an [OSE](#) running a client operating system.

Clustered HPC Application means a high performance computing applications that solves, in parallel, complex computational problems, or a set of closely related computational problems. Clustered HPC Applications divide a computationally complex problem into a set of jobs and tasks which are coordinated by a job scheduler, such as provided by Microsoft HPC Pack, or similar HPC middleware, which distributes these in parallel across one or more computers operating within an HPC cluster.

Cluster Node means a device that is dedicated to running [Clustered HPC Applications](#) or providing job scheduling services for [Clustered HPC Applications](#).

Core Factor means a numerical value associated with a specific [Physical Processor](#) for purposes of determining the number of Licenses required to license all of the [Physical Cores](#) on a [Server](#).

Cycle Harvesting Node means a device that is not dedicated to running [Clustered HPC Applications](#) or job scheduling services for [Clustered HPC Applications](#).

External Connector License means a License assigned to a [Server](#) dedicated to Customer's use that permits access to the corresponding version of the server software or earlier versions of the server software by [External Users](#).

External Users means users that are not either Customer's or its Affiliates' employees, or its or its affiliates' onsite contractors or onsite agents.

Hardware Thread means either a [Physical Core](#) or a hyper-thread in a [Physical Processor](#).

High Performance Computing (HPC) Workload means a workload where the server software is used to run a [Cluster Node](#) and is used in conjunction with other software as necessary to permit security, storage, performance enhancement and systems management on a [Cluster Node](#) for the purpose of supporting the [Clustered HPC Applications](#).

Hyper-V Container is a feature of Windows Server that utilizes a virtual operating system environment. Each Hyper-V Container is considered to be one [Virtual OSE](#).

Instance means an image of software that is created by executing the software's setup or install procedure or by duplicating an existing [Instance](#).

License means the right to download, install, access and use a Product.

Licensed Device means a single physical hardware system to which a License is assigned. For purposes of this definition, a hardware partition or blade is considered to be a separate device.

License Mobility through Software Assurance Partner means an entity identified at <http://www.microsoft.com/licensing/software-assurance/license-mobility.aspx> and authorized by Microsoft to host customers' software on shared servers.

Licensed Server means a single [Server](#), dedicated to Customer's use, to which a [License](#) is assigned. For purposes of this definition, a hardware partition or blade is considered to be a separate Server.

Licensed User means the single person to whom a [License](#) is assigned.

Management License (ML) means a License that permits management of one or more [OSEs](#) by the corresponding version of the server software or any earlier version of the server software. There are two categories of Management Licenses: Server Management License and Client Management License. There are three types of Client Management Licenses: User, OSE and device. A User Management License permits management of any [OSE](#) accessed by one user; an OSE Management License permits management of one [OSE](#) accessed by any user; a device Management License (Core CAL or Enterprise CAL Suite) permits management of any [OSE](#) on one device.

Management License Equivalent License means a User SL identified in a Product's "Management License" table, or a [CAL](#) suite or [SL](#), as identified in the Management License Equivalent Licenses Table, [Appendix A](#), as applicable. A [CAL](#) suite is a Management License Equivalent License only if Customer purchased the license after the Server Products' Date Available or if Customer had active SA coverage as the Date Available.

Managing an OSE means to solicit or receive data about, configure, or give instructions to the hardware or software that is directly or indirectly associated with the [OSE](#). It does not include discovering the presence of a device or [OSE](#).

Operating System Environment (OSE) means all or part of an operating system Instance, or all or part of a virtual (or otherwise emulated) operating system Instance which enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and instances of applications, if any, configured to run on the operating system Instance or parts identified above. A physical hardware system can have one [Physical OSE](#) and/or one or more [Virtual OSEs](#).

Physical Core means a core in a [Physical Processor](#).

Physical OSE means an [OSE](#) that is configured to run directly on a physical hardware system. The operating system Instance used to run hardware virtualization software or to provide hardware virtualization services is considered part of the [Physical OSE](#).

Physical Processor means a processor in a physical hardware system.

Primary User means the user who uses a [Licensed Device](#) more than 50% of the time in any 90 day period.

Production Environment means any Physical or Virtual OSE running a production workload or accessing production data, or [Physical OSE](#) hosting one or more [Virtual OSEs](#) running production workloads or accessing production data.

Qualifying Third Party Device means a device that is not controlled, directly or indirectly, by Customer or its Affiliates (e.g., a third party's public kiosk).

Running Instance means an [Instance](#) of software that is loaded into memory and for which one or more instructions have been executed. (Customer "Runs an Instance" of software by loading it into memory and executing one or more of its instructions.) Once running, an Instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.

SL means subscription [License](#) that allows access to software or a hosted service for a defined period of time.

Server means a physical hardware system capable of running server software.

Server Farm means a single data center or two data centers each physically located either in time zones not more than four hours apart, or within the EU or EFTA. A data center can be moved from one Server Farm to another, but not on a short-term basis. (EU is European Union; EFTA is European Free Trade Association).

Step-up means a license purchased in addition to (and associated with) a previously acquired base license. For any Step-up User SL not appearing individually in the OST, the license terms applicable to the equivalent full User SL apply.

Virtual Core means the unit of processing power in a virtual hardware system. A Virtual Core is the virtual representation of one or more hardware threads.

Virtual OSE means an [OSE](#) that is configured to run on a virtual hardware system.

Web Workload (also referred to as "[Internet Web Solutions](#)") are publicly available web pages, websites, web applications, web services, and/or POP3 mail serving. For clarity, access to content, information, and applications served by the software within an Internet Web Solution is not limited to Customer's or its affiliates' employees.

Software in Internet Web Solutions is used to run:

- web server software (for example, Microsoft Internet Information Services), and management or security agents (for example, the System Center Operations Manager agent);
- database engine software (for example, Microsoft SQL Server) solely to support Internet Web Solutions; or
- the Domain Name System (DNS) service to provide resolution of Internet names to IP addresses as long as that is not the sole function of that instance of the software.

Windows Server Container is a feature of Windows Server software.

Windows Software Components means components of Windows software included in a Product. Microsoft .NET Framework, Microsoft Data Access Components, PowerShell software and certain .dlls related to Microsoft Build, Windows Identity Foundation, Windows Library for JavaScript, Debghelp.dll, and Web Deploy technologies are all Windows Software Components.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Appendix A – CAL/ML Equivalent Licenses

Rights to access server software running on Customer's [Licensed Servers](#) or to [Manage OSEs](#) are available under [CAL](#) suites and Online Services [SLs](#). If a cell is shaded blue in a server's row, the [CAL](#) suite or [SL](#) in that column satisfies the [License](#) requirement for access to (or management of) that [Server](#) Product's base or additive functions. [CAL](#) suites must be purchased after the Product's Date Available or have active SA coverage on such date to satisfy access requirements for the current version of the [Server](#) Product.

Servers	Office 365 Enterprise				Core CAL					Enterprise CAL					Enterprise Mobility + Security		Secure Productive Enterprise	
	E1	E3	E4	E5	Suite	Bridge O365	Bridge Intune	Bridge O365+Intune	Bridge EMS	Suite	Bridge O365	Bridge Intune	Bridge O365+Intune	Bridge EMS	E3	E5	E3	E5
Exchange Server 2016 Standard																		
Base																		
Additive																		
Exchange Server 2016 Enterprise																		
Base																		
Additive																		
SharePoint Server 2016																		
Base																		
Additive																		
Microsoft Audit and Control Management Server 2013																		
Base																		
Skype for Business Server 2015																		
Base																		
Additive(Ent)																		
Additive (Pls)																		
Windows MultiPoint Server 2016 Premium (Academic only)																		
Base																		
Additive																		
Windows Server 2016 Standard																		
Base																		
Additive (RMS)																		
Additive (MIM)																		
Windows Server 2016 Data Center																		
Base																		
Additive (RMS)																		
Additive (MIM)																		
Advanced Threat Analytics 2016																		
Management																		
System Center Configuration Manager 1606																		
Management																		

Note: Office 365 Education E1 and Office 365 Nonprofit E1 do not satisfy the License requirement for access to (or management of) the Products in this table. A license for the Core CAL and Enterprise CAL Suite includes with active SA coverage provides rights equivalent to System Center Endpoint Protection 1606. A license for the Enterprise CAL Suite with active SA coverage provides rights equivalent to Data Loss Prevention and Exchange Online Protection.

Appendix B – Software Assurance

Purchasing Software Assurance

There are three different levels of commitment Customer may select when purchasing SA, which may vary by program. Customer can:

1. Commit to attaching SA on all platform products.
2. Commit to attaching SA on all purchases under a particular Product pool (Applications, Systems or Servers), referred to as Software Assurance Membership (SAM).
3. Purchase SA on individual Products without making any commitment to expanding SA to other Products.

SA must be acquired at the time of acquiring the [License](#) or upon renewal of an existing SA term. Unless otherwise stated, only licenses for the latest version of a Product are eligible for SA. In the case of a transfer of perpetual [Licenses](#), the transferee may acquire SA for such transferred [Licenses](#) within 30 days from the date of transfer and provided that the transferor maintained active SA for the [Licenses](#) up until the date of transfer.

Customers may have the option to acquire SA for certain licenses purchased from the Retail channel (full packaged product) or from an Original Equipment Manufacturer (OEM), as described in the table below. Under Open Value, this option applies only to non-Organization-wide/ Company-wide products. Under Enterprise Agreements, it applies only to Additional Products within 90 days from the date of purchase. Customers who acquire SA for OEM or retail licenses have the option of installing and using the Volume Licensing software for the current version at any time.

Pool	Full Packaged Products	OEM	Programs
Application Pool	N/A	SA available only as outlined below	Applies to Open License, MPSA, Select, Select Plus and non Organization wide under Open Value and Additional Products under Enterprise Agreements. It does not apply to Enterprise Products under Open Value and Enterprise Agreements.
Server Pool	SA available	SA available	

Customers who acquire Microsoft Office Professional 2016 from an OEM may acquire SA for Microsoft Office Standard 2016 in the Open License programs, Select and Select Plus programs, and non Company-wide under Open Value within 90 days from the date of OEM purchase.

Enterprise Agreement customers who transitioned to an Online Service or who purchased a From SA subscription License in lieu of renewing SA may reattach SA to a License at anniversary or renewal without purchasing a new License. SA must be ordered for that License for the remainder of the enrollment term. SA coverage may not exceed the quantity of perpetual Licenses for which SA was current at the time of any prior transition or renewal and may not be reattached to transferred Licenses.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Renewing Software Assurance

Renewing Coverage under the Same Agreement

Terms for renewing SA under the same program agreement by which it was initially ordered are contained Customer's volume licensing agreements. Customers may renew SA without the need to simultaneously order a License as long as the SA coverage has not expired. In addition, the following terms apply to specific programs as noted:

Open License

SA coverage ordered under an Open License authorization number ends upon expiration of that number. To renew, Customer must submit a renewal order for SA within 90 days after their authorization number expiration date.

Enterprise Agreement

To renew SA coverage under the same enrollment under an Enterprise Agreement, Customer must sign a new 2011 or later Enterprise Enrollment and Agreement (if they have not already), and must submit a renewal order for SA (as applicable) for 1) all Enterprise Products, Application Platform Products, Core Infrastructure Products and Additional Products they wish to renew and 2) any Online Services, accounting for transitions (if applicable).

Enrollment for Application Platform

EAP customers who have previously deferred [Licenses](#) via SA prior L SKUs must buyout their [Licenses](#) before they can renew SA.

Renewing Coverage from a Separate Agreement

Customer may renew SA for any Product if Customer has obtained a perpetual [License](#) and SA for that Product under a previous agreement in the same Volume Licensing Program, provided that 1) Customer's new agreement enrollment, or order (for MPSA) must be effective no later than the day following the date of expiration of the previous agreement or enrollment, and 2) the SA renewal order must be placed prior to the expiration of prior SA coverage, unless such coverage is being renewed from an Open License Agreement. In that case, Customers have 90 days from the expiration to place the order.

Customer may also renew SA from one Volume Licensing program into a different Volume Licensing Program. For Enterprise Products originally purchased under a program with a company-wide coverage requirement, this exception applies only if the customer is renewing SA into the MPSA or a program with a company-wide coverage requirement for Enterprise Products. For Agreement versions 2008 and prior, as long as coverage is renewed within 30 days (90 days if renewing from Open License program), customers will be deemed to have SA coverage during any period of time between when their expiring SA coverage lapsed and when the new coverage begins.

Renewing Software Assurance Coverage for Client Access Licenses (CALs) and Client Management Licenses (MLs)

Transitioning between User and Device CALs: Customers renewing SA for CALs can switch between User and Device. This transition does not change the CAL edition (i.e. Standard to Enterprise).

Transitioning between User and OSE Client MLs: Customers renewing SA for client MLs can switch between User and OSE.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Migration License for Discontinued or End-of-Life Products

“Qualifying License,” as used here, refers to a [License](#) with SA coverage as of the date specified and for the Product identified in the product entry referencing this section.

“Migration License,” as used here, refers to rights granted in the Product Entry referencing this section.

Unless stated otherwise in the Product Entry:

- Customer may upgrade to and use software under a Migration License in place of software covered by the Qualifying License. The Customer may not use software under both licenses simultaneously.
- Migration Licenses are granted on 1:1 for each of Customer’s Qualifying Licenses.
- If Customer acquired perpetual rights to use software under a Qualifying License, the rights to use software acquired under the Migration License are likewise perpetual; otherwise, rights acquired under a Migration License expire when the underlying Qualifying License expires.
- Upon expiration of SA coverage on the Qualifying License, Customer may acquire SA for the same version and edition of the Product covered by the Migration License, without the need to first acquire separate new Licenses. This option does not apply to customers buying licenses under subscription programs (e.g., Enterprise Subscription Agreements or Open Value Subscription agreements).
- Customer may not transfer Migration Licenses separately from Qualifying Licenses.
- Subsequently acquired licenses for the same discontinued Product under the same enrollment term under an Enterprise or Enterprise Subscription Agreement, Open Value Subscription or Enrollment for Education Solutions, as part of Customer’s scheduled true-up process are also Qualifying Licenses for purposes of the license grant. Coverage for Products under subscription agreements must be continuous.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Software Assurance Benefits

Most SA Benefits are available across each Product Pool, as described in the table below. Active SA for any qualifying Product qualifies Customer for the benefits shown in the table below. Some benefits are awarded based on Customer’s SA spend on a given set of qualifying products within a pool. For these purposes, “SA spend” is not literally Customer’s actual dollars spent, but is an approximation of what Customer has spent on SA coverage for those Products under its Select or Enterprise Enrollment, Select Plus registration or Open agreement (For example, SA only purchases and the SA component of L&SA purchases). For customers under subscription programs, it is an approximation of the total dollars Customer has spent licensing those Products under its enrollment or agreement. Software Assurance Membership (“SAM”) is required for some benefits. Customer’s access and rights to use their SA benefits, generally expires upon expiration of their SA coverage, unless otherwise noted below or in the Product Entries. The benefits are subject to change and may be discontinued at any time without notice. Availability of benefits varies by program, region, fulfillment options and language.

Benefits	Applications Pool	Systems Pool	Server Pool
New Version Rights	X	X	X
Office Online, Office Online Server	X		
Planning Services	X		X
Enterprise Source Licensing Program		X	
Enterprise Sideload		X	
Windows Thin PC		X	
Microsoft Desktop Optimization Pack (MDOP)		X	
Windows Virtual Desktop Access (VDA)		X	
Training Vouchers	X	X	
E-Learning	X	X	X
Home Use Program	X		
24x7 Problem Resolution Support	X	X	X

Extended HotFix Support	X	X	X
Microsoft Dynamics CustomerSource			X
Step-Up License	X		X
System Center Global Service Monitor			X
Servers – Disaster Recovery Rights			X
License Mobility			X
Servers – Self Hosted Applications			X
Windows SA per User Add-on Purchase Rights		X	
Windows to Go		X	
Virtualization Rights for Windows and Windows Embedded Desktops		X	

New Version Rights

Customer may upgrade to the latest version of an available Product. If Customer acquires perpetual Licenses through SA, it may deploy new version upgrades for those Licenses after SA coverage has expired, but only to versions released during the active SA coverage. Use of the new version is subject to the [License Terms](#) for that version.

Calculating Software Assurance Benefits Points

Entitlements are calculated on a points-based system for the following benefits:

- Planning Services
- Training Vouchers
- 24x7 Problem Resolution Support (Phone) in MPSA only

Software Assurance Benefits points are calculated based on the number of qualifying licenses, applicable pools, and the points associated with qualifying products as listed in the following table. Points cannot be combined across agreements, enrollments, or Purchasing Accounts to qualify for additional points. Reduction of points as a result of returns and other billing adjustments, where allowed, may result in the loss of entitlements during the present or future entitlement periods.

Office Applications and Server Licenses	Points
Office Application Pool Products (including Office suites, Project Standard and Professional, Visio Standard and Professional), Windows Desktop Operating System Products, Microsoft Dynamics AX Task CAL, Microsoft Dynamics AX Store Server ¹ , Microsoft Dynamics AX Functional CAL ¹ , and Microsoft Dynamics 365 CAL ¹	1
Windows Server Standard (2-pack Core License), System Center Standard Server Management License (2-pack Core License)	5
Windows Server Datacenter (2-pack Core License), System Center Datacenter Server Management License (2-pack Core License)	10
SQL Server Standard edition, Windows Server Standard edition, System Center Standard Server Management License (2-processor), Visual Studio Professional with MSDN, Visual Studio Test Professional with MSDN, and Microsoft Dynamics AX Enterprise CAL	25
SQL Server Enterprise edition, SQL Server Business Intelligence, Windows Server Enterprise edition and Visual Studio Enterprise with MSDN	50
SQL Server Data Center edition, SQL Parallel Data Warehouse, Windows Server Datacenter edition, Microsoft Dynamics AX Standard Commerce Core Server, and System Center 2012 Datacenter Server Management License (2-processor)	75

Note: For SQL CALs, see the CAL Suites table in this section

¹ For Microsoft Dynamics 365 for Sales On-premises CAL and Microsoft Dynamics 365 for Customer Service On-premises CAL, 2 points are awarded

Office Online Services and Office Online Server

Users of a device licensed with the qualifying applications may access Office Online services and Office Online Server for editing documents from the [Licensed Device](#). The Primary User of the [Licensed Device](#) may access Office Online services and Office Online Server for editing documents from any device.

Qualifying Desktop Application	Office Online rights
Office Standard Office Professional Plus Office for Mac Standard	Office Online for Office 365 Office Online Server

Users must also be licensed for SharePoint Online or OneDrive for Business plans to access Office Online service.

Planning Services

Customers (other than those purchasing through Academic Programs) with a Company-wide commitment or SAM in the Application and Server Pools are eligible for this benefit. The Planning Services benefit provides qualifying customers with pre-determined customized service offerings.

Qualified customers receive a number of Planning Services days based on the number of SA Benefit points from qualifying licenses. The number of days Customer receives for the available Planning Services offerings are combined into a pool of Planning Services days.

Office Applications and Server Licenses	Points
Office Application Pool Products (including Office suites, Project Standard and Professional, Visio Standard and Professional), Microsoft Dynamics AX Task CAL, Microsoft Dynamics AX Store Server ¹ , Microsoft Dynamics AX Functional CAL ¹ , and Microsoft Dynamics 365 CAL ¹	1
SQL Server Standard edition, Windows Server Standard edition, Microsoft Dynamics CRM Server 2013 and Microsoft Dynamics CRM Server 2015, System Center 2012 Standard Server Management License (2-processor), Visual Studio Professional with MSDN, and Visual Studio Test Professional with MSDN, and Microsoft Dynamics AX Enterprise CAL	25
SQL Server Enterprise edition, SQL Server Business Intelligence, Windows Server Enterprise edition and Visual Studio Enterprise with MSDN	50

SQL Server Data Center edition, SQL Parallel Data Warehouse, Windows Server Datacenter edition, Microsoft Dynamics AX Standard Commerce Core Server, and System Center 2012 Datacenter Server Management License (2-processor)	75

Note: For SQL CALs, see the CAL Suites table in this section

¹ For Microsoft Dynamics 365 for Sales On-premises CAL and Microsoft Dynamics 365 for Customer Service On-premises CAL, 2 points are awarded

The total points Customer is eligible for defines the Planning Services Days entitlements as shown below:

Office Applications and/ or Server Licenses Points	200-499	→1,999	→3,999	→29,999	→49,999	→99,999	→199,999	→399,999	→599,999	600,000+
Office Planning Services Days	1	3	5	10	15	20	30	40	50	75

Core CAL Suite and SQL CAL SA coverage counts as one (1) point toward the thresholds in the first column below, Enterprise CAL Suite SA coverage counts as two (2) points toward the thresholds in the first column below:

CAL Suites	200-3,999	→9,999	→99,999	→299,999	→599,999	→600,000+
Office Planning Services Days	1	3	5	7	10	12

Customers may select from available Planning Service offerings provided by qualified Microsoft Partners or Microsoft Affiliates. A list of available services can be found at <http://www.microsoft.com/licensing/software-assurance/planning-services-overview.aspx>.

The list of available services and associated service levels may change at any time. Qualified Providers will provide customers with an outline of the available Scope of Work for each of the above service offerings. Upon request customers can also convert (and un-convert) unused Training Voucher days (see the Training Voucher benefit) at a rate of three Training Voucher days into one Planning Service Day, if they (i) are currently eligible for the Training Voucher benefit, (ii) have activated their Training Voucher benefit, and (iii) have at least 3 unclaimed training days from Training Voucher benefit available for conversion.

- Planning Services may be delivered to Customer by qualified Microsoft Partners or Microsoft Affiliates. Services provided under vouchers are provided under an agreement between Customer and the Qualified Provider Customer can view the list of Qualified Providers here: <http://directory.partners.extranet.microsoft.com/psbproviders>
- Planning Services engagements provide services that covers a pre-determined scope of work that result in a high level deployment plan; the actual deployment of the software cannot be included.
- Planning Services vouchers can only be redeemed by the customer who qualified for the benefit.
- Planning Services vouchers may not be exchanged for cash, monies or other valuable considerations.
- Reduction of qualifying SA coverage as a result of returns and other billing adjustments, where allowed, may lower Customer's Planning Services entitlement days.
- Voucher types may not be combined. Planning Services engagements must not exceed the maximum specified duration per engagement type.
- Vouchers are only valid with qualified Providers for the specific service type for which the voucher is being redeemed.
- Vouchers must be assigned during the SA coverage period.
- Vouchers will expire 180 days from the date of voucher assignment, independent of SA coverage expiration. All services must be delivered (voucher redeemed) prior to voucher expiration. Vouchers that expire prior to SA coverage expiration will return to the available Planning Services pool of days. The tables above show service days available based on a full 3-year enrollment or agreement. Customers who purchase SA coverage for one-year will receive one third of the stated number of service days. Customers who purchase SA coverage for two-years will receive two thirds of the stated number of service days.

Completed deliverables submitted by the Qualified Provider at the end of the engagement to Microsoft may be used by Microsoft for quality assurance purposes and may be shared with Customer's Microsoft account team for that purpose.

Enterprise Source Licensing Program

Customers with 10,000 or more licensed desktops with SA coverage in the systems pool may be eligible to access to Microsoft Windows source code for internal development and support. Academic programs are eligible for the Microsoft Research Source Licensing Program.

Training Vouchers

Customers (other than those purchasing through Academic Programs) with a Company-wide commitment or SAM in the application or systems Product pools are eligible for Microsoft Training Vouchers granting a specific number of training days as described below.

Program	Office System Application Pool products	Systems Pool
Open Value	2 days per 50 licenses (maximum 20 days)	1 day per 50 licenses (maximum 10 days)
SAM 1-249	2 days per 50 licenses or points	1 day per 50 licenses or points
SAM 250-2,399	20 days per eligible enrollment or Purchasing Account	10 days per eligible enrollment or Purchasing Account
SAM 2,400-5,999	30 days*	15 days*
SAM 6,000-14,999	50 days*	25 days*
SAM 15,000 – 29,999	110 days*	55 days*
SAM 30,000 – 49,999	160 days*	80 days*

SAM 50,000 – 99,999	250 days*	125 days*
SAM 100,000 – 199,999	400 days*	200 days*
SAM 200,000 – 399,999	600 days*	300 days*
SAM 400,000 – 599,999	800 days*	400 days*
SAM 600,000 +	1400 days*	700 days*

*Number of days per eligible enrollment, agreement, or Purchasing Account

- Services provided under vouchers are provided under an agreement between Customer and the qualified Microsoft Learning Partner.
- Courses delivered in an accelerated format require voucher days equivalent to the number of course days for the course delivery set in the SATV Voucher Validation and Reservation System.
- The voucher is only redeemable for days of instructor-led training with qualified Microsoft Learning Partners on approved courses. Custom courses (other than accelerated delivery of approved courses, custom courses compiled solely from approved courses or pre-approved exceptions based on systems issues or pilot programs) are not eligible for coverage by these vouchers.
- Vouchers cannot be used to cover any fees related to a customer not showing up for a reserved course.
- Vouchers may only be redeemed by the individual approved by the customer to use the voucher.
- Vouchers may not be exchanged for cash, monies or other valuable considerations.
- Vouchers must be assigned during the SA coverage period.
- Vouchers will expire 180 days from the date of voucher assignment. Vouchers that expire prior to SA coverage expiration will return to the available Training Voucher pool of days.
- One Training Voucher day is equal to the equivalent of one training session day.
- Vouchers may be used to reserve training with only one qualified Microsoft Learning Partner at a time.
- Reduction of the number of qualifying licenses for which SA is acquired as a result of returns and other billing adjustments, where allowed, may lower Customer's Training Vouchers service level eligibility.
- The table above shows training credits available based on a full 3-year enrollment or agreement. Customers who purchase SA coverage for one-year will receive one third of the stated number of training credits. Customers who purchase SA coverage for two-years will receive two thirds of the stated number of training credits.

E-Learning

This benefit varies by Applications, Systems, and Servers. Eligible customers will receive one access code (for Applications, Systems, and/or Servers) per qualifying enrollment/agreement. Customers with qualifying Server Products are eligible to use hosted E-Learning Server courses but not SCORM-compliant content. Customers with Office 365 Pro Plus are eligible to use hosted Office 365 related E-Learning courses only (SCORM-compliant content is not eligible).

The maximum number of users for which a Customer may use the E-Learning training is equal to the number of licensed copies of qualifying products that Customer has enrolled in SA. Customers must designate one user for each qualifying license. Access cannot be transferred from one user to another.

Home Use Program

Customer's employees, who are users of the licensed qualifying applications identified in the table below may acquire a single [License](#) for the corresponding Home Use Program software, to be installed on one device (either a PC or a Mac, specific to the software that is purchased). Academic Select (without SAM), Academic Select Plus (without SAM), and Academic Open programs are not eligible for this benefit.

Home Use Licenses expire with termination of employment, termination or expiration of SA coverage for the copy of the corresponding desktop application that employee uses at work, if the employee is no longer a user of the licensed copy of the software, or upon the employee's installation and use of any prior or later version of that desktop application pursuant to a Home Use Program license.

The terms of use for the Home Use Program software are between Microsoft and Customer's employee and are accessed through the Home Use Program website.

Microsoft assumes no responsibility for compliance with any employment-benefit, tax or reporting obligation that either Customer or its employees may have.

Qualifying Desktop Application	Corresponding Home Use Program License
Office Standard 2010/2013/2016 Office Professional Plus 2010/2013/2016 Office for Mac Standard 2011/Office 2016 for Mac Standard	Office Professional Plus 2016 HUP and Office 2016 for Mac Home & Business with Lync DL HUP
Access 2010/2013/2016 Excel 2010/2013/2016 PowerPoint 2010/2013/2016 InfoPath 2010/2013/2016 Lync 2010/2013/2015 OneNote 2010/2013/2016 Outlook 2010/2013/2016 Publisher 2010/2013/2016 Skype for Business 2015	Office Professional Plus 2016 HUP and Office 2016 for Mac Home & Business with Lync DL HUP

Word 2010/2013/2016	
Visio Standard 2010/2013 /2016 Visio Professional 2010/2013/2016	Visio Professional 2016 HUP
Project Standard 2010/2013/2016 Project Professional 2010/2013/2016	Project Professional 2016 HUP

For more information, including information on the future availability of additional Home Use Program software, refer to <http://www.microsoft.com/licensing>.

Microsoft may terminate a customer's participation in the Home Use Program, immediately and without notice, in connection with unauthorized access to or licensing through the Home Use Program website in connection with that customer's program code.

24x7 Problem Resolution Support

Customers (other than those purchasing through Academic Programs) with SA coverage are eligible for 24x7 Problem Resolution Support.

24x7 Problem Resolution Support provides assistance for problems with specific symptoms encountered while using Microsoft products. Microsoft will make reasonable efforts to assist Customer with support requests in a manner consistent with Microsoft Product Support policies. Microsoft reserves the right to refuse unreasonable requests for support services, and may refer Customers to an additional service level agreement which may require an additional charge.

Products that are currently in Mainstream Support as set forth in Microsoft's Support Lifecycle Policy are eligible for 24x7 Problem Resolution Support. Microsoft can add support for new Products or discontinue support for existing Products. Microsoft will notify Customer if Customer's implementation of Microsoft products cannot be supported. If Customer does not modify the implementation to make it effectively supportable within 30 days after the notice, Microsoft will not be obligated to provide additional support services for that implementation.

An assisted break-fix support request, also known as an incident, is defined as a single support issue and the reasonable effort needed to resolve it. A single support issue is a problem that cannot be broken down into subordinate issues. If a problem consists of subordinate issues, each shall be considered a separate incident. In certain situations, Microsoft may provide a modification to the commercially available Microsoft Product software code to address specific critical problems ("Hotfix(es)") in response to an assisted break-fix support request. Hotfixes are designed to address Customer's specific problems and are not regression tested.

Phone Support Incident Awards for all programs except MPSA

The number of permitted phone support incidents varies by customer based upon their SA spend and payment option. SA-spend-based incidents are earned based on server and desktop SA spend under a qualifying Select or Enterprise enrollment, Select Plus registration, Open Value Agreement or Open License Authorization number. Microsoft will award one incident for each Server SA or CAL SA spend of at least \$20,000. Microsoft will award one incident for each Systems Pool or Applications Pool SA spend of at least \$200,000. The table below shows the approximate currency equivalents for SA-spend-based awards for agreements based in currencies other than USD. Due to the fluctuation of exchange rates, this table is subject to change.

Currency Name	Currency Code	Server / CAL - Incident Award Increments	IW / Client - Incident Award Increments
US Dollar	USD	\$20,000	\$200,000
Australian Dollar	AUD	30,000	300,000
Canadian Dollar	CAD	27,000	270,000
Swiss Franc	CHF	S Fr. 33,000	S Fr. 330,000
China Renminbi	CNY	CRC 165,000	CRC 1,650,000
Danish Krone	DKK	kr 160,000	kr 1,600,000
EURO	EUR	21,500	215,000
UK Pound	GBP	£13,500	£135,000
Japanese Yen	JPY	JPY 2,400,000	JPY 24,000,000
Korean Won	KRW	KWD 24,000,000	KWD 240,000,000
Norwegian Krone	NOK	kr 165,000	kr 1,650,000
New Zealand Dollar	NZD	35,000	350,000
Swedish Krona	SEK	kr 200,000	kr 2,000,000
New Taiwan Dollar	TWD	NTD 700,000	NTD 7,000,000
India Rupee	INR	INR 1,000,000	INR 10,000,000
Russian Ruble	RUB	RUB 660,000	RUB 6,600,000

Phone Support Incidents that have not been used will expire at the expiration of SA coverage. Phone Support Incidents may not be transferred between enrollments or agreements.

Access to local phone support is available during business hours found on the website <http://support.microsoft.com/gp/saphone>. After-hours phone support may be provided through regional and international support centers. After-hours phone support can only be used to initiate

business critical support requests. Business hours are determined on a region-by-region basis. Phone support assistance is not available in all languages in all regions.

Phone Support Incidents Awards for MPSA

The number of permitted phone support incidents varies based upon Customer's SA benefits points earned. If Customer has SA coverage on at least one qualifying Server software Product, Customer is entitled to a complimentary incident. The number of phone support incidents to which Customer is entitled is based on the total calculated points earned through Customer's Purchasing Account, as shown below (refer to the 'Calculating Software Assurance Benefits Points' section of this document for details of how SA Benefits points are calculated):

Pool	Points per phone support incident
Applications and Systems (combined)	2,000
Server	400
CAL	400

Incidents are entitled over the term of the SA coverage and are available for use from the start of Customer's SA coverage, regardless of whether or not Customer has chosen to spread payments. Purchases made after the initial order will trigger recalculation of the incidents awarded and the annual allotment. Phone Support Incidents that have not been used will expire at the expiration of SA coverage. Phone Support Incidents may not be transferred between Purchasing Accounts.

Access to local phone support is available during business hours found on the website <http://support.microsoft.com/gp/saphone>. After-hours phone support may be provided through regional and international support centers. After-hours phone support can only be used to initiate business critical support requests. Business hours are determined on a region-by-region basis. Phone support assistance is not available in all languages in all regions.

Web-Based Incidents

Customers (other than Academic Select License, Select Plus for Academic, Academic Open License, Campus and School Agreement, Open Value Subscription – Education Solutions, and Open License) with Standard, Enterprise and Datacenter Editions of server software covered with SA have access to electronic web-based Problem Resolution Support services on an as needed basis. Access to the electronic support sites is available 24 hours per day, 7 days a week, though responses will occur during Business Hours. Incidents initiated via the Web then converted to phone resolution by Customer will count against the available phone incident balance upon resolution. Incidents initiated via the Web then followed up via phone by Microsoft will not count against the available phone incident balance if resolution continues on Web, email and other electronic means.

SA is required for both server software and related CALs for Web Support incidents. Customers may only submit web-based Problem Resolution Support requests on those licensed copies of server software covered with SA.

Support Contacts

The number of permitted support contacts varies by Volume Licensing program and number of licenses covered under SA, as shown below. Contacts must be named individuals and can include individuals from outside Customer's organization. However, an organization, department or group name may not be listed as a contact.

Benefits	OL	OV	S/S+: EA Level A	S/S+: EA Level B	S/S+: EA Level C & MPSA	S/S+: EA Level D
# of Problem Resolution Phone Support Contacts	As Needed	As Needed	As Needed	As Needed	As Needed	As Needed
# of Authorized Web Support Contacts	NA	1	2	3	8	16

Service Level for Software Assurance Customers

Estimated response times by severity level and Customer's responsibilities are defined in the following table:

Severity	Situation	Microsoft's Expected Response	Customer's Expected Response
A. Submission via phone	Critical business impact: Customer's business has significant loss or degradation of services	1st call response in 2 hours or less based on support offering Microsoft Resources at Customer site as required.	Allocation of appropriate resources to sustain continuous effort on a 24x7 basis Rapid access and response from change control authority Management notification
B. Submission via phone	Moderate business impact: Customer's business has moderate loss or degradation of services but work can reasonably continue in an impaired manner.	1st call response in 4 hours or less based on support offering Effort during Business Hours only	Allocation of appropriate resources to sustain Business Hours continuous effort Access and response from change control authority within 4 Business Hours
C. Submission via phone or web	Minimum business impact: Customer's business is substantially	1st response in one business day or less based on support offering	Accurate contact information on case owner

	functioning with minor or no impediments of services.	Effort during Business Hours only	Responsive within one business day.

1 Contact Microsoft representative for local business hours.

2 Microsoft may need to downgrade the severity level if Customer is not able to provide adequate resources or responses to enable Microsoft to continue with problem resolution efforts.

Conversion of Software Assurance 24x7 Problem Resolution Support Incidents to Premier Support Services

With the exception of MPSA, Customers may convert SA 24x7 Problem Resolution Support Incidents (SA PRS Incidents, or “SAB”) to Premier Problem Resolution Support (PRS) hours or Dedicated Support Engineer (DSE) hours (applicable for reactive support activities only).

These services are for use consistent with their Premier Service plan at the time of transfer. The conversion is based on a local rate calculation that will be provided by their Premier Account Team. Customers may be required to purchase additional Support Account Management hours before converting SA PRS incidents. SA PRS incidents that are converted to Premier are considered Premier Problem Resolution Support hours and are subject to the Premier Services Description. Once converted, incidents cannot be returned to Customer’s SA allowance.

Additional Business Provisions

SA spend may not be combined across Select or Enterprise enrollments, Select Plus registrations, Purchasing Accounts, or Open Value Agreements to qualify for additional awards. Spending within each enrollment, agreement, or Purchasing Accounts will be used to determine the award for that enrollment, agreement, or Purchasing Accounts.

Reduction of SA Spend as a result of returns and other billing adjustments, where allowed, may result in the loss of Support eligibility or Phone incident awards during the present or future award periods.

SCE Eligibility

Customers who have an SCE with a minimum annual average SA spend of \$250,000 on total of qualifying products in either the Application Platform or the CIS Suite and who have an active Premier Services Agreement are eligible for Unlimited 24x7 Problem Resolution Support (PRS) incidents. The two eligible SCE components qualify separately for Unlimited 24x7 Problem Resolution Support. Products listed below, that are currently in Mainstream or Extended Support as set forth in Microsoft’s Support Lifecycle Policy in line with a Customer’s Premier contract, are included in this benefit.

The qualifying Application Platform Products are:

- SQL Server (Standard, Standard Core, Enterprise Core, Business Intelligence and Parallel Data Warehouse and CALs)
- BizTalk Server (Standard, Enterprise, and Branch)
- Office SharePoint Server

The qualifying products from the Core Infrastructure Component are:

- CIS Suite Datacenter (Windows Server Datacenter and System Center Datacenter)
- CIS Suite Standard (Windows Server Standard and System Center Standard)

The table below lists the SA spend threshold conversions for agreements based in currencies other than USD. Due to the fluctuation of exchange rates, this table is subject to change without notice.

Currency	Currency Code	Minimum Annual Average SA spend to qualify for Unlimited 24x7 PRS
US Dollar	USD	250,000
Australian Dollar	AUD	375,000
Canadian Dollar	CAD	337,500
Swiss Franc	CHF	412,500
China Renminbi	CNY	2,062,500
Danish Krone	DKK	2,000,000
EURO	EUR	268,750
UK Pound	GBP	168,750
Japanese Yen	JPY	30,000,000
Korean Won	KRW	300,000,000
Norwegian Krone	NOK	2,062,500
New Zealand Dollar	NZD	437,500
Swedish Krona	SEK	2,500,000
New Taiwan Dollar	TWD	8,750,000
India Rupee	INR	12,500,000
Russian Ruble	RUB	8,250,000

When committed annual average SA spend on qualifying Application Platform and/or Core Infrastructure products eligible for Unlimited 24x7 PRS is higher than \$250,000, Microsoft will not award incidents based on actual SA spend on these products. If Customer becomes eligible for

Unlimited 24x7 PRS midstream, any incident previously awarded based on SA spend and not consumed will be subtracted from Customer's balance. Unlimited 24x7 PRS incidents cannot be converted to Premier Problem Resolution Support hours or incidents.

Parallel Data Warehouse Eligibility

Customers who acquire licenses for SQL Server Enterprise Edition, deploy Parallel Data Warehouse ("PDW") and have an active Premier Services Agreement are eligible for Unlimited 24x7 PRS incidents, regardless of being enrolled in an SCE or their SCE spend.

While all qualifying customers will receive an unlimited number of 24x7 PRS incidents, the number of permitted support contacts to manage Unlimited 24x7 PRS does vary by size of the SA spend. All eligible customers are entitled to at least four authorized contacts plus one additional contact per every additional \$125,000 of SA spend under their SCE or VL program (s) under which they purchased licenses for SQL Server Enterprise Edition, deploy PDW. For agreements in foreign currencies, eligible customers are entitled to at least four authorized contacts plus one additional contact for each incremental SA spend amount equivalent to \$125,000 of annual average SA spend in the applicable foreign currency. See table below:

The following table applies to customers who have an SCE or have licenses for PDW:

Annual Average SA spend	Permitted support contacts
\$250,000 - \$374,999	4
\$375,000 - \$499,999	5
\$500,000 - \$624,999	6
\$625,000 - \$749,999	7
\$750,000 - \$874,999	8

The number of permitted support contacts for MPSA is 8 regardless of SA spend. The Unlimited 24x7 PRS benefit only includes Problem Resolution Services. Any time spent by the Technical Account Manager (TAM) or the Designated Support Engineer (DSE) on the resolution of the incident will be accounted for under Customer's Premier Services Agreement.

Note: Customers currently licensed for PDW maintain this benefit as detailed in the [June 2016 Product Terms](#).

Extended HotFix Support

Extended Hotfix Support is available to customers who have signed a Premier or Essential Support agreement and have purchased SA under the following programs:

- Customers (other than those purchasing through Academic Programs) with SAM coverage for Applications Pool qualify for Extended Hotfix Support for Application pool products.
- Customers (other than those purchasing through Academic Programs) with SAM coverage for Systems pool qualify for Extended Hotfix Support for Windows desktop operating system and/or Windows Embedded operating system (with SAM coverage on a Windows Embedded product).
- Customers (other than those purchasing through Academic Programs) with SA on at least one server product qualify for Extended Hotfix Support for Server products. The following server products are covered: Microsoft Exchange Server, Microsoft SQL Server, System Center, and Windows Server.

Extended Hotfix Support is a benefit for older software versions that have transitioned from Mainstream to Extended Support. For customers who have signed a Premier or Essential Support agreement, the annual fees for an Extended Support contract are waived. Customers are still responsible for the fees for individual Hotfixes.

Step-Up License Availability

The Step-Up License must be acquired, and is valid only when acquired, under the same volume licensing agreement and enrollment (if any), under which SA coverage for the qualifying product was acquired. Customer's right to the use of software under a Step-Up License is conditioned on their having and retaining a License for the qualifying product. Customers' perpetual rights under the Step-Up License supersede and replace the underlying License for the qualifying product. For more details, refer to the Enterprise Edition [Step-Up License Volume Licensing Brief](#):

<http://www.microsoft.com/licensing>

Step Up From	Step Up To
BizTalk Server Branch	BizTalk Server Standard
BizTalk Server Branch	BizTalk Server Enterprise
BizTalk Server Standard	BizTalk Server Enterprise
Core CAL Suite	Enterprise CAL Suite
Core Infrastructure Server Suite Standard	Core Infrastructure Server Suite Datacenter
Desktop Education w/ Core CAL	Desktop Education w/ Enterprise CAL Suite
Desktop School w/ Core CAL	Desktop School w/ Enterprise CAL Suite
Exchange Server Standard	Exchange Server Enterprise
Forefront TMG Standard	Forefront TMG Enterprise
Microsoft Dynamics 365 for Team Members On-premises CAL	Microsoft Dynamics 365 for Sales On-premises CAL
Microsoft Dynamics 365 for Team Members On-premises CAL	Microsoft Dynamics 365 for Customer Service On-premises CAL
Office Standard	Office Professional Plus

Professional Desktop	Enterprise Desktop
Project Standard	Project Professional
SQL Parallel Data Warehouse Core	SQL Server Enterprise Core
SQL Server Standard Core	SQL Server Enterprise Core
SQL Server Standard	SQL Server Business Intelligence
System Center Standard	System Center Datacenter
Visio Standard	Visio Professional
Visual Studio Professional with MSDN	Visual Studio Enterprise with MSDN
Visual Studio Test Professional with MSDN	Visual Studio Enterprise with MSDN
Windows Server Standard	Windows Server Datacenter

Servers – Disaster Recovery Rights

For each [Instance](#) of eligible server software Customer runs in a [Physical OSE](#) or [Virtual OSE](#) on a [Licensed Server](#), it may temporarily run a backup [Instance](#) in a [Physical OSE](#) or [Virtual OSE](#) on either, another one of its [Servers](#) dedicated to disaster recovery, or, for [Instances](#) of eligible software other than Windows Server, on Microsoft Azure Services, provided the backup [Instance](#) is managed by Azure Site Recovery to Azure. The [License Terms](#) for the software and the following limitations apply to Customer's use of the backup [Instance](#).

The backup [Instance](#) can run only during the following exception periods:

- For brief periods of disaster recovery testing within one week every 90 days;
- During a disaster, while the production [Server](#) being recovered is down; and
- Around the time of a disaster, for a brief period, to assist in the transfer between the primary production server and the disaster recovery [Server](#).

In order to use the software under disaster recovery rights, Customer must comply with the following terms:

- The [OSE](#) on the disaster recovery [Server](#) must not be running at any other times except as above.
- The [OSE](#) on the disaster recovery [Server](#) may not be in the same cluster as the production [Server](#).
- Other than backup instances run on Microsoft Azure Services, Windows Server [License](#) is not required for the disaster recovery [Server](#) if the following conditions are met:
 - The Hyper-V role within Windows Server is used to replicate [Virtual OSEs](#) from the production [Server](#) at a primary site to a disaster recovery [Server](#).
 - The disaster recovery [Server](#) may be used only to
 - run hardware virtualization software, such as Hyper-V,
 - provide hardware virtualization services,
 - run software agents to manage the hardware virtualization software,
 - serve as a destination for replication,
 - receive replicated [Virtual OSEs](#), test failover,
 - await failover of the [Virtual OSEs](#), and
 - run disaster recovery workloads as described above.
 - The disaster recovery [Server](#) may not be used as a production [Server](#).
- Use of the software backup [Instance](#) should comply with the [License Terms](#) for the software.
- Once the disaster recovery process is complete and the production [Server](#) is recovered, the backup [Instance](#) must not be running at any other times except those times allowed here.
- Maintain SA coverage for all [CALs](#), External Connector licenses and Server [Management Licenses](#) under which it accesses the backup instance and manage the [OSEs](#) in which that software runs.
- Customer's right to run the backup [Instances](#) ends when Customer's Software Assurance coverage ends.

License Mobility

License Mobility Across Server Farms

Under License Mobility Across Server Farms, Customer may reassign any of its [Licenses](#) which are designated as having License Mobility and for which it has SA to any of its [Licensed Servers](#) located within the same [Server Farm](#) as often as needed. Customer may also reassign these [Licenses](#) from one [Server Farm](#) to another, but not on a short-term basis (i.e., not within 90 days of the last assignment). Products used for Self-Hosting may be used at the same time under License Mobility Across Server Farms rights.

License Mobility through Software Assurance

Under License Mobility Through Software Assurance (SA), Customer may move its licensed software to shared servers under any of its [Licenses](#) which are designated as having [License Mobility](#) for which it has SA, subject to the requirements below. Products used for Self-Hosting may be used at the same time under License Mobility through SA rights, subject to the limitations of the Self-Hosting License Terms.

Permitted Use:

With License Mobility through SA, Customer may:

- Run its licensed software on shared servers;

- Access that software under access licenses and for which it has SA, and under its User and Device SLs that permit access to the Products;
- Manage its [OSEs](#) that it uses on shared servers; and/or
- Manage its [OSEs](#) that it uses on its servers using software that it runs on shared servers.

Requirements:

To use License Mobility through SA, Customer must:

- Run its licensed software and manage its [OSEs](#) on shared servers under the terms of its volume licensing agreement;
- Deploy its [Licenses](#) only with Microsoft Azure Platform Services or qualified [License Mobility through Software Assurance Partner](#); and
- Complete and submit the License Mobility Validation form with each [License Mobility through Software Assurance Partner](#) who will run its licensed software on their shared servers.

Customer may move its licensed software from shared servers back to its Licensed [Servers](#) or to another party's shared servers, but not on a short term basis (not within 90 days of the last assignment). Customer may also move [Instances](#) run or [OSEs](#) managed under a particular [License](#) from shared servers in one [Server Farm](#) to its shared servers in another [Server Farm](#), but not on a short-term basis (not within 90 days of the last assignment). [OSEs](#) managed under the same License must be in the same [Server Farm](#). Customer agrees that it will be responsible for third parties' actions with regard to software deployed and managed on its behalf. Except as provided below, the [License Terms](#) applicable to the Product together with the License Mobility through SA terms govern its use. The License Mobility through SA terms supersede any conflicting License terms for a Product when License Mobility through SA is used. Some Products, as outlined below, have different use rights for shared servers under License Mobility through SA:

License Model	Product/Product Type	License	Permitted Number of: OSEs or Cores per License
Per Core/CAL	External Connector Licenses	Each External Connector License with active SA coverage	1 OSE per license
Server/CAL	SQL Server	Each Server License with active SA coverage	1 OSE per license
Per-Core	All eligible Products	Each Core License with active SA coverage	One virtual core (subject to the product use rights including the requirement of a minimum of 4 cores per OSE)
Management Servers	System Center 2012 R2 Standard	Each Management License with active SA coverage	2 Managed OSEs per Licensed Server
Management Servers	System Center 2012 R2 Datacenter	Each Management License with active SA coverage	10 Managed OSEs per Licensed Server

Fail-over Rights

For Products that are also granted [Fail-Over Rights](#), Customer may run passive fail-over [Instances](#) on the qualifying shared servers in anticipation of a fail-over event. The number of licenses that otherwise would be required to run the passive fail-over [Instances](#) must not exceed the number of licenses required to run the corresponding production [Instances](#) on the same partner's shared servers.

Servers – Self Hosted Applications

Self-Hosted Applications means those Products for which Self-Hosted rights apply.

Despite any terms to the contrary in Customer's volume licensing agreement including the Product Terms, Customer may run licensed copies of Self-Hosted Applications that interact directly or indirectly with its software to create a unified solution ("Unified Solution") and permit third parties to use it, subject to the terms below.

Requirements

Customer must have the required Microsoft [Licenses](#) and SA for:

- the Self-Hosted Applications run as part of the Unified Solution; and
- all access [Licenses](#) used to make the Unified Solution available to External Users.

All Microsoft software used to create and deliver the Unified Solution must be:

- licensed through a Volume Licensing program; and
- eligible for [Self Hosting](#) under these License Terms.

If Customer delivers the Unified Solution from shared servers, Customer may not use Windows Server (nor Remote Desktop Services External Connector License or any other Windows Server access license) as a Self-Hosted Application. Instead, Customer must use Windows Server software licensed through a License Mobility through Software Assurance Partner or Customer's Services Provider Licensing Agreement, or under another Microsoft Volume Licensing offering permitting use on shared servers. Other Products used in a Unified Solution delivered from shared servers must have License Mobility through Software Assurance.

Customer's software must:

1. add significant and primary functionality to the Self-Hosted Applications that are part of the Unified Solution (dashboards, HTML editors, utilities, and similar technologies alone are not a primary service and/or application of a Unified Solution);
2. be the principal service and/or application of the Unified Solution, and must not allow direct access to the Self-Hosted Applications by any end user of the Unified Solution;
3. be delivered to end users over the Internet, a telephone network, or a private network from servers under the day to day control of Customer or a third party other than the end user of the Unified Solution (the Unified Solution may not be loaded onto the end user's device); and
4. be owned, not licensed, by it, except that its software may include non-substantive third party software that is embedded in, or operates in support of, its software.

All use of the Self-Hosted Applications remains governed by the [License Terms](#) for those products. Customer may not transfer [Licenses](#) acquired under its volume licensing agreement except as permitted in that agreement.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Appendix C – Professional Services

The Professional Services available through Microsoft Volume Licensing are described below.

Microsoft Premier Support Offerings

Area ¹	Premier Core	Premier Foundation	Premier Standard	Premier Plus
Support Account Management	X	X	X	X
Account Profiling & Reporting	Monthly	Monthly	Monthly	Monthly
Support Assistance (Hours annually allocated)	Up to 10 hours	Up to 10 hours +1 Health Check +1 Workshop	Up to 120 hours	Up to 160 hours
Problem Resolution Support (PRS) (annually allocated)	Up to 40 hours	Up to 30 hours	Up to 80 hours	Up to 140 hours
24x7 Critical Situation Escalation Management (Severity Level 1)	X	X	X	X
Rapid Onsite Support	X	X	X	X
Proactive Information Services	X	X	X	X
Microsoft Premier Online	X	X	X	X
Add-on Hours	Packs of 20	Packs 20	Packs of 20	Packs of 20

¹Business Hours are defined locally.

Severity	Situation	Microsoft's Expected Response	Customer's Expected Response
1. Submission via phone only	Catastrophic business impact: Complete loss of a core (mission critical) business process and work cannot reasonably continue Needs immediate attention	1st call response in 1 hour or less Microsoft's Resources at customer site as soon as possible. Continuous effort on a 24x7 basis Rapid Escalation within Microsoft to Product teams Notification of Microsoft's Senior Executives	Notification of Customer Senior executives Allocation of appropriate resources to sustain continuous effort on a 24x7 basis ² Rapid access and response from change control authority
A. Submission via phone only	Critical business impact: Significant loss or degradation of services Needs attention within 1hour	1st call response in 1 hour or less Microsoft's Resources at Customer site as required. Continuous effort on a 24x7 basis Notification of Microsoft's Senior Managers	Allocation of appropriate resources to sustain continuous effort on a 24x7 basis ² Rapid access and response from change control authority Management notification
B. Submission via phone or web	Moderate business impact: Moderate loss or degradation of services but work can reasonably continue in an impaired manner. Needs attention within 2 Business Hours ¹	1st call response in 2 hours or less Effort during Business Hours ¹ only	Allocation of appropriate resources to sustain Business Hours ¹ continuous effort Access and response from change control authority within 4 Business Hours ¹
C. Submission via phone or web	Minimum business impact: Substantially functioning with minor or no impediments of services. Needs attention within 4 Business Hours ¹	1st call response in 4 hours or less Effort during Business Hours ¹ only	Accurate contact information on case owner Responsive within 24 hours

¹Business Hours are defined locally.

²Microsoft may need to downgrade the severity level if Customer is not able to provide adequate resources or responses to enable Microsoft to continue with problem resolution efforts.

Associated Business Rules

All Professional Services provide support for commercially released, generally available Microsoft Products (unless specifically excluded on the Microsoft Premier On-Line Web site or the Microsoft Support Lifecycle Web site). Professional Services will generally be charged on an hourly basis, provided remotely, and in English (unless another language is available). Professional Services will be provided in the country in which the VL agreement is signed. On-Site visits are not pre-paid and are subject to resource availability. All Professional Services not consumed on an annual basis will be forfeited. Upon Customer request, Microsoft may access Customer's system via remote dial-in to analyze problems.

Microsoft Digital Advisory Services Offerings

The Digital Advisory Services offerings contain the following components which will be provided for each year of the Customer's Enterprise Agreement:

Area	Enterprise Strategy Connect	Enterprise Strategy Foundation	Enterprise Strategy Portfolio
SKU Product Family	9TH-xxxx	8A3-xxxx	9RO-xxxx

Service Delivery	Up to 400 hours in aggregate of a Microsoft Digital Advisor and the Enterprise Service Delivery Team	Up to 800 hours in aggregate of a Microsoft Digital Advisor and the Enterprise Service Delivery Team	Up to 1600 hours in aggregate of a Microsoft Digital Advisor and the Enterprise Service Delivery Team
Services Delivery Plan (SDP)			
Digital Advisory Network			
Digital Advisory Services Library			
Digital Advisory Capacity (SKU Product Family: 9RS-xxxx)	200 hours of Digital Advisor (can be added to any engagement)		

Digital Advisory Service Modules

The Digital Advisory engagement includes one or more Digital Advisory service modules, as documented in the Service Delivery Plan.

Services Out of Scope

The Professional Services in a Digital Advisory engagement do not include problem resolution or break fix support, review of non-Microsoft source code, or technical or architectural consultation beyond the deliverables as described in a Services Delivery Plan. For any non-Microsoft source code, Microsoft's Professional Services will be limited to analysis of binary data only, such as a process dump or network monitor trace.

Customer Responsibilities

Customer agrees to cooperate with Microsoft as part of the Digital Advisory engagement, including but not limited to making Customer's representatives, IT staff, and resources available to Microsoft, providing accurate and complete information, and timely completing responsibilities assigned to Customer by Microsoft. Where onsite visits of Microsoft Consultants are mutually agreed and not pre-paid, Customer is responsible for reasonable travel and living expenses.

Sales Productivity Accelerator Offerings

Sales Productivity Accelerator Overview

The Sales Productivity Accelerator is a service provided by Microsoft Services over the course of a four (4)-week-term to deliver a fixed-scope implementation of Microsoft Dynamics 365.

The Sales Productivity Accelerator includes the following deliverables:

- **Service Delivery Plan:** created by a Microsoft Consultant to meet the customer's business goals and objectives.
- **Workshops:** will devote up to a total of sixteen (16) hours for workshops:
 - Up to two (2) discovery workshops, to explore and define key use cases and business requirements, as provided by Customer, to configuration settings;
 - Up to four (4) design review workshops during the Build phase.
- **Reporting:** One (1) native Microsoft Dynamics 365 dashboard with up to four (4) native components and two (2) Excel Power View Reports using Power BI Pro5 configured for up to two (2). The reports display up to two (2) interactive charts per entity with data sourced from Microsoft Dynamics 365.
- **Configuration:** Microsoft Dynamics 365 will be configured to support up to a total of ten (10) users. During this time, Microsoft will devote up to sixty-four (64) hours to configure the lead thru opportunity processes, 3 security roles, 3 persona's leveraging out of the box security roles, SharePoint and Yammer integration with Microsoft Dynamics 365.
- **Testing:** will devote up to twenty-six (26) hours devoted to up to two (2) tests (e.g., System Test & UAT).
- **Training and Knowledge Transfer:** Provide one (1) product-oriented training for Customer's users, for up to a total of four (4) hours.
- **Deployment Support:** Provide up to forty (40) hours of deployment and go-live support (week 4) subject to the pre-determined project scope and requirements.

Customer Responsibilities

Customer agrees to cooperate with Microsoft as part of the Sales Productivity Accelerator service, including but not limited to making Customer's representatives, IT staff, and resources available to Microsoft, providing accurate and complete information, and timely completing responsibilities assigned to Customer by Microsoft. Where onsite visits of Microsoft Consultants are mutually agreed and not pre-paid, Customer is responsible for reasonable travel and living expenses.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Appendix D – Program Agreement Supplemental Terms

The terms and conditions below apply to Customer's volume licensing agreement, as noted.

Supplemental Terms for Select Plus Program

Select Plus requires a minimum order quantity of 500 points per pool during the first year. This order quantity requirement may be waived if a Qualified Contract is supplied.

Price Levels in Select Plus

Customer's prices are based upon agreement between Customer and Customer's reseller. However, Microsoft provides reseller with the following price and point criteria to help guide reseller to end customer pricing:

Select Plus Price Level-Commercial	Annual Point Minimums per Pool
A	500
B	4,000
C	10,000
D	25,000

Definition of Management for Qualified Devices

If Customer's volume licensing agreement refers to the Product Terms, the Product List, or the PUR for defining managed Qualified Devices, the following terms apply. Customer "manages" any device on which it directly or indirectly controls one or more operating system environments. For example, Customer manages any device:

- it allows to join its domain, or
- it authenticates as a requirement to use applications while on its premises, or
- it installs agents on (e.g., anti-virus, antimalware or other agents mandated by the Customer's policy), or
- to which it directly or indirectly applies and enforces group policies, or
- on which it solicits or receives data about, and, configures, or gives instructions to hardware or software that is directly or indirectly associated with an operating system environment, or
- it allows to access a virtual desktop infrastructure (VDI) outside of Windows SA, Microsoft Intune (Device) or Windows Virtual Desktop Access Roaming Rights.

A device that accesses a VDI under Roaming Rights only or utilizes Windows To Go on a Qualifying Third Party Device off the Customer's premises only, and is not managed for other purposes as described here, is not considered "managed" for purposes of this definition.

Online Services in the Open Programs

Under the Open License, Open Value, and Open Value Subscription programs, the subscription period for Online Services starts at the time of product key activation and not the time of order. Once the product key is activated, Microsoft will not accept return requests submitted by Microsoft's partners.

Customer qualifies for the Open Value program with a minimum purchase of 5 licenses. Online Services User Subscription Licenses (User SLs) can be counted toward the minimum quantity of 5 licenses. However, 5 User SLs alone does not meet the minimum for Open Value Organization Wide and Open Value Subscription. For OV Organization Wide and OV Subscription the initial order must include a minimum of 5 Desktop Platform or Desktop Component Licenses in addition to any User SLs.

Supplemental Terms for Professional Services – Legacy Agreements

Customer's right to use of any consulting and support services Microsoft performs ("Professional Services") purchased from the Product Terms are governed by (1) customer's volume licensing agreement, and (2) any master-level Microsoft Services agreement customer may have in place at the time of purchase. In the event of a conflict, the most current Professional Services agreement controls. If Customer's master agreement for volume licensing is a Microsoft Business Agreement version dated prior to September, 2007 or otherwise does not include terms for Professional Services, and Customer has not signed any other master-level Microsoft Services agreement, the following supplemental terms apply to any Professional Services purchased and used by Customer.

Use, Ownership, and License Rights

Fixes

If Microsoft provides Product Fixes, modifications or enhancements, or their derivatives, either released generally (such as Product service packs) or to address a specific issue for Customer (collectively, "Fixes"), such Fixes are licensed under the same terms as the Product to which it applies. If the Fixes are not provided for a specific product, any use terms Microsoft provides with the Fixes will apply.

Pre-Existing Work

All rights in any computer code or non-code based written materials developed or otherwise obtained independent of the Professional Services provided to Customer ("Pre-Existing Work") shall remain the sole property of the party providing it. Each party may use, reproduce and modify the other party's Pre-Existing Work only as needed to perform obligations related to Professional Services. Except as may be otherwise expressly agreed by the parties in writing, upon payment in full Microsoft grants Customer a non-exclusive, perpetual, fully paid-up license to use, reproduce and modify (if applicable) any Microsoft Pre-existing Work provided as part of a Services Deliverable, solely in the form delivered to Customer, and solely for Customer's internal business purposes. The license to Microsoft's Pre-Existing Work is conditioned upon Customer's compliance with the terms of Customer's volume licensing agreement.

Services Deliverables

Any computer code or materials other than Products or Fixes that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services are considered Services Deliverables. Upon payment in full for the Professional Services, Microsoft grants Customer a non-exclusive, non-transferable, perpetual license to reproduce, use, and modify the Services Deliverables solely for Customer's internal business purposes, subject to the terms and conditions governing the Professional Services and Customer's volume licensing agreement.

Use of technical information from Professional Services

Microsoft may use any technical information it derives from providing Professional Services for problem resolution, troubleshooting, product functionality enhancements, in Fixes, and for Microsoft's knowledge base. Microsoft agrees not to identify Customer or disclose any of Customer's Confidential Information as part of such use.

Open Source License Restrictions

Customer must not install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property to obligations beyond those included in these Professional Services terms or Customer's volume licensing agreement.

Affiliates' Rights

Customer may sublicense the rights to use Services Deliverables to its Affiliates, but Customer's Affiliates may not sub-license these rights. Customer is liable for ensuring its Affiliates' compliance with these Professional Services terms and Customer's volume licensing agreement.

Warranties and Limitations of Liability

Warranty for Professional Services

Microsoft warrants that it will perform the Professional Services with professional care and skill. If Microsoft fails to do so and Customer notifies Microsoft within 90 days of the date the Professional Services were performed, then Microsoft will, as the sole remedy for the breach of the warranty, either re-perform the Professional Services or return the price Customer paid for them. **Except for the limited warranty above, Microsoft provides no other warranties or conditions and disclaims any other express, implied or statutory warranties, including warranties of quality, title, non-infringement, merchantability and fitness for a particular purpose.**

Limitation of Liability

Microsoft's liability for direct damages will be limited to the amounts Customer was required to pay for the Professional Services. In the case of services provided free of charge, or code Customer is authorized to redistribute to third parties without separate payment to Microsoft, Microsoft's liability is limited to direct damages up to U.S. \$5,000. **In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, including loss of use, loss of profits, or interruption of business, however caused or on any theory of liability in relation to the Professional Services. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations; or (2) violation of the other party's intellectual property rights.**

[Table of Contents](#) / [Glossary](#) / [Index](#)

Appendix E – Promotions

Azure Compute Capacity Promotion

From November 1, 2015 to March 31, 2017, the Azure Compute Capacity promo offers discounts on A, D, and G Series Compute instances as non-coterminous 12 month subscriptions.

New Customer Azure Monetary Commitment Offer

A new or renewing Enterprise Agreement or Campus and School Agreement customer who purchases at least 21 Azure Monetary Commitment units per month between November 1, 2016 and June 30, 2017 will be eligible to receive a one-time Azure Monetary Commitment credit equal to up to 25% of the Azure Monetary Commitment that customer consumes during the first 3 months of the agreement term. The Monetary Commitment credit will be added to the customer's Monetary Commitment balance 4 calendar months after the effective date of the new or renewed agreement. Any portion of the Monetary Commitment credit that has not been consumed by the next Enrollment anniversary will expire and be forfeited.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Appendix F - Storage Array Terms

Availability

The Storage Array is available for delivery in the following geographies only: Argentina, Australia, Austria, Bahrain, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Kenya, Kuwait, Lebanon, Macau, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Nigeria, Norway, Pakistan, Peru, Philippines, Poland, Portugal, Puerto Rico, Qatar, Romania, Russia, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, South Korea, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, Ukraine, United Kingdom, United States, Vietnam.

Shipment and Title

Shipping terms for orders placed are: (i) FCA (Incoterms 2010) Supplier Shipping dock; (ii) Microsoft will pre-pay and invoice freight to Customer; and (iii) for shipments outside the United States, Customer is responsible for clearing the goods for import and paying all import costs including duties, taxes, and other clearance charges. Microsoft will supply the Storage Array to the Customer on a No Charge basis and title for the Storage Array and the risk of loss will pass to Customer upon delivery to the carrier and completion of export formalities at the point of origin. All scheduled shipment dates are estimates only. The Storage Array will be shipped to the address provided by Customer using the StorSimple online form (provided separately). For US transactions, Microsoft has remitted sales tax on the value of the Storage Array(s) based upon the ship-to address provided by Customer for the delivery of the Storage Array(s). For US and Canada transactions, the address used for the shipment of the Storage Array(s) is used strictly for purposes of shipping the device to Customer and does not impact any other ship-to (or Tax Address) provided on Customer's volume license agreement used for purposes of charging sales tax to Customer on purchases made under that volume license agreement.

Storage Array Software

Microsoft grants Customer a non-exclusive, non-transferrable, limited license to use the Software that runs in the Storage Array ("Storage Array Software") only in connection with Customer's use of the Storage Array. Customer's use of the Storage Array Software is subject to the terms of Customer's volume license agreement governing Software, and Microsoft reserves all other rights.

Restrictions

Customer may not use the Storage Array Software for comparisons or "benchmarking" except for Customer's internal purposes or publish or disclose the results thereof.

Certain Third Party Open Source Software

The Storage Array Software may be distributed with certain independent code (e.g., firmware) that is licensed under the GNU General Public License ("GPL"), the GNU Library/Lesser General Public License ("LGPL"), the Apache License Version 2.0 ("Apache License") and/or other open-source licenses ("Open-Source Code"). Any such Open-Source Code is identified in the Third Party Software Notices located at: <http://go.microsoft.com/fwlink/?LinkId=627000>, and is licensed to Customer in accordance with the applicable open-source licenses.

Activation/Consent for Internet-based Services

Activation associates the use of the Storage Array Software with a specific device. During activation and subsequent use of the device, the Storage Array Software may send information about the Storage Array Software and device to Microsoft. This information includes the version, language, and product key of the Storage Array Software, Customer's Internet protocol address, operating system, browser and name, the version of the Storage Array Software Customer is using, and the language code of the Storage Array running the Storage Array Software. Microsoft uses this information to make the Internet-based services available to Customer. By using the Storage Array and Storage Array Software, Customer consents to the transmission of this information to Microsoft.

Storage Array Software Updates

The update service for Storage Array Software will allow Customer to download available updates manually, or opt-in to receiving updates automatically. Available updates from Microsoft will be licensed by Microsoft and any third party updates will be licensed by the applicable third party.

Limited Hardware Warranty

Microsoft warrants that the Storage Array hardware will not malfunction due to a defect in materials or workmanship under ordinary commercial use as described in the applicable product documentation for a period of ninety (90) days from the date of delivery to Customer. If it does not and Customer notifies Microsoft within the warranty term, Microsoft will repair or replace it (at Microsoft's election) at no charge. This is the only warranty Microsoft gives for the Storage Array, and Customer waives any breach of warranty claims not made during the warranty period. This warranty does not cover problems caused by accident, abuse or use in a manner inconsistent with Customer's volume license agreement or the product documentation and it is void if the Storage Array is opened or modified, damaged by use with Non-Microsoft Products, or damaged by maintenance or repair performed by anyone other than Microsoft or a Microsoft authorized vendor. **Microsoft provides no other warranties or**

conditions and disclaims any other express, implied or statutory warranties, including without limitation, warranties of quality, title, non-infringement, merchantability, and fitness for a particular purpose.

Indemnification. Defense of third party claims

Microsoft will defend Customer against any claims made by an unaffiliated third party that a Storage Array infringes its patent, copyright or trademark or makes unlawful use of its Trade Secret, subject to the terms of the Customer's volume license agreement regarding defense of third party claims.

Limitation of Liability

For any claim related to a Storage Array, each party's maximum, aggregate liability to the other is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the applicable Storage Array. **In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, including loss of use, loss of profits, or interruption of business, however caused or on any theory of liability. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations; (2) defense obligations; or (3) violation of the other party's intellectual property rights.**

U.S. Export Control Laws

The Storage Arrays are subject to the provisions in Customer's volume licensing agreement regarding U.S. export jurisdiction.

Collection of Diagnostic Information

Microsoft may collect information to help Microsoft diagnose problems related to the Storage Array and provide potential solutions. If Microsoft receives indication of a potential problem, it may collect information from the Storage Array through the Azure StorSimple Management Service. The types of information collected may include files that help describe or identify the problem, such as operational logs, whether the problem occurred in the hardware or software, the type and severity of the problem, and device status. Microsoft will not collect memory dumps, keys, passwords, or data that a Customer stores on the Storage Array. Microsoft uses the information to improve the Storage Array and related services, and may also use it to improve third party hardware and firmware included as part of the Storage Array. To the extent that Microsoft provides its hardware vendor with specific information, Microsoft will only provide the information in an anonymized data format unless Microsoft obtains Customer's explicit consent. Microsoft will provide this information for the purpose of resolving an identified hardware related issue. To learn more about privacy for the Storage Array, refer to <https://www.microsoft.com/en-us/privacystatement>.

Government Use

Customer understands that in exchange for purchasing one or more StorSimple Monetary Commitment Offerings, Microsoft will provide the Storage Array and StorSimple Support to Customer at no additional charge. Microsoft waives any and all entitlement to compensation from Customer for such Storage Array or StorSimple Standard Support. Microsoft intends that the provision of the Storage Array and StorSimple Standard Support to Customer without charge will fully comply with applicable gift, ethics and other laws and regulations related to gratuitous goods and services. Microsoft intends that the provision of Storage Arrays and StorSimple Standard Support shall be for the sole benefit and use of Customer and not for the personal use or benefit of any individual government employee.

[Table of Contents](#) / [Glossary](#) / [Index](#)

Index

- Access 2016, 22
- Advanced Threat Analytics 2016 Client Management License per OSE, 13
- Advanced Threat Analytics 2016 Client Management License per User, 13
- Apple Macintosh, 40
- Azure Active Directory Basic (User SL), 51
- Azure Active Directory Premium Plan 1 (User SL), 51
- Azure Active Directory Premium Plan 2 (User SL), 51
- Azure Active Professional Direct Support, 51
- Azure Active Standard Support, 51
- Azure App Service Plan, 51
- Azure Information Protection Premium Add-on, 60
- Azure Information Protection Premium Plan 1 (User SL), 51
- Azure Information Protection Premium Plan 1 Add-on (User SL), 51
- Azure Information Protection Premium Plan 2 (User SL), 51
- Azure Information Protection Premium Plan 2 Add-on, 51
- Azure Site Recovery, 83
- Azure Site Recovery (to Customer Owned Site), 51
- Bing Maps Asset Management for Windows, 65
- Bing Maps Asset Management Platform Monthly Subscription, 65
- Bing Maps Enterprise Fee Monthly Subscription, 65
- Bing Maps Internal Website Usage 100K Transactions Monthly Subscription, 65
- Bing Maps Internal Website Usage 500K (and higher) Transactions Monthly Subscription, 65
- Bing Maps Known 5K User Monthly Subscription, 65
- Bing Maps Known Per User Monthly Subscription, 65
- Bing Maps Light Known 500 User Monthly Subscription, 65
- Bing Maps Light Known 5K User Monthly Subscription, 65
- Bing Maps Public Website Usage 100K Transaction Monthly Subscription, 65
- Bing Maps Public Website Usage 500K (and higher) Transactions Monthly Subscription, 65
- BizTalk Server, 81
- BizTalk Server 2013 R2, 14
- BizTalk Server 2016 Branch Edition, 13
- BizTalk Server 2016 Branch IDC, 13
- BizTalk Server 2016 Enterprise Edition, 13
- BizTalk Server 2016 Standard Edition, 13
- BizTalk Server 2016 Standard Edition IDC, 14
- BizTalk Server Branch, 82
- BizTalk Server Enterprise, 82
- BizTalk Server Standard, 82
- Business Productivity Online Deskless Suite, 61
- CIS Suite Datacenter, 81
- CIS Suite Standard, 81
- Communicator for Mac 2011, 24
- Core CAL, 32, 54, 59, 77, 82
- Core CAL Bridge for Office 365, 60
- Core CAL Suite, 14
- Core CAL Suite Bridge for Enterprise Mobility+ Security, 15
- Core CAL Suite Bridge for Microsoft Intune, 14
- Core CAL Suite Bridge for Office 365, 14, 54
- Core CAL Suite Bridge for Office 365 and Microsoft Intune, 14, 54
- Core Infrastructure Server Suite Datacenter, 16, 82
- Core Infrastructure Server Suite Standard, 16, 82
- Enterprise CAL, 32, 54, 60, 63, 77, 82
- Enterprise CAL Bridge for Enterprise Mobility + Security, 15
- Enterprise CAL Bridge for Enterprise Mobility + Security From SA, 15
- Enterprise CAL Bridge for Office 365, 60
- Enterprise CAL Suite, 15
- Enterprise CAL Suite Bridge for Microsoft Intune, 15
- Enterprise CAL Suite Bridge for Office 365, 15, 54
- Enterprise CAL Suite Bridge for Office 365 and Microsoft Intune, 15, 54
- Enterprise CAL Suite Bridge for Office 365 From SA, 15
- Enterprise Mobility + Security, 54, 60
- Enterprise Mobility + Security E3, 15, 54
- Enterprise Mobility + Security E3 Add-on, 54
- Enterprise Mobility + Security E3 From SA, 54
- Enterprise Mobility + Security E5, 15, 54
- Enterprise Mobility + Security E5 Add-on, 54
- Enterprise Mobility + Security E5 From SA, 54
- Enterprise Mobility + Security From SA, 54
- Excel 2016, 22
- Excel 2016 for Mac, 23
- Exchange Hosted Archive, 62
- Exchange Online Archiving for Exchange Online, 62
- Exchange Online Archiving for Exchange Server, 15, 62
- Exchange Online Kiosk, 62
- Exchange Online Plan 1, 25, 62
- Exchange Online Plan 1 Add-on, 60, 62
- Exchange Online Plan 1A for Alumni, 62
- Exchange Online Plan 2, 25, 62
- Exchange Online Protection, 15, 62
- Exchange Server, 53
- Exchange Server 2013, 24
- Exchange Server Enterprise, 82
- Exchange Server Enterprise 2016, 24
- Exchange Server Enterprise 2016 CAL, 24
- Exchange Server Standard, 82
- Exchange Server Standard 2016, 24
- Exchange Server Standard 2016 CAL, 24
- Forefront Identity Manager 2010 - Windows Live Edition, 18
- Forefront Identity Manager 2010 R2, 21
- Forefront Identity Manager 2010 R2 - Windows Live Edition, 18
- Forefront TMG Enterprise, 82
- Forefront TMG Standard, 82
- Forefront United Access Gateway 2010, 16
- HPC Pack, 48
- Import Service for Office 365, 62
- IoT Suite Predictive Maintenance Plan 1, 51
- IoT Suite Predictive Maintenance Plan 2, 51

IoT Suite Remote Monitoring Plan 1, 51	Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 2
IoT Suite Remote Monitoring Plan 2, 51	Standard Acceptance testing, 56
Live Meeting Professional, 27	Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 3
Live Meeting Standard, 27	Premier Acceptance testing, 56
Lync 2013, 22	Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 4
Lync for Mac 2011, 23, 65	Standard Performance testing, 56
Lync Server 2010, 27	Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 5
Lync Server 2013, 27	Premier Performance testing, 56
Microsoft Azure Platform Services, 84	Microsoft Dynamics 365 for Operations, Enterprise edition (User SL), 55
Microsoft Azure Services, 51, 83	Microsoft Dynamics 365 for Operations, Enterprise edition Add-on (Device and User SL), 55
Microsoft Azure StorSimple Plan 8100 Renewal, 51	Microsoft Dynamics 365 for Operations, Enterprise edition From SA (Device and User SL), 55
Microsoft Azure StorSimple Plan 8600 Renewal (no device), 51	Microsoft Dynamics 365 for Project Service Automation, Enterprise edition (User SL), 55
Microsoft Azure StorSimple Plan with Device (8100 device), 51	Microsoft Dynamics 365 for Sales On-premises CAL, 18, 57, 82
Microsoft Azure StorSimple Plan with Device (8600 device), 51	Microsoft Dynamics 365 for Sales, Enterprise edition, 19
Microsoft Azure StorSimple Premium Support, 51	Microsoft Dynamics 365 for Sales, Enterprise edition, 55
Microsoft Azure StorSimple Standard Support, 51	Microsoft Dynamics 365 for Sales, Enterprise edition (User SL), 55
Microsoft Azure StorSimple Standard Support to Premium Support, 51	Microsoft Dynamics 365 for Team Members On-premises CAL, 18, 82
Microsoft Cloud App Security (User SL), 51	Microsoft Dynamics 365 for Team Members, Enterprise edition, 19, 20
Microsoft Cloud App Security K (User SL), 52	Microsoft Dynamics 365 for Team Members, Enterprise edition (User SL), 55
Microsoft Dynamics 365 CAL, 76	Microsoft Dynamics 365 for Team Members, Enterprise edition Add-on (User SL), 56
Microsoft Dynamics 365 Enhanced Support, 56	Microsoft Dynamics 365 for Team Members, Enterprise edition From SA (User SL), 56
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Database Storage, 56	Microsoft Dynamics 365 Plan 1, Enterprise edition (User SL), 55
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Non-Production Instance, 56	Microsoft Dynamics 365 Plan 2 Enterprise edition Add-on (User SL), 55
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Portal, 56	Microsoft Dynamics 365 Plan 2, Enterprise edition (User SL), 55
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Portal Page Views, 56	Microsoft Dynamics 365 Plan 2, Enterprise edition From SA (User SL), 55
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Production Instance, 56	Microsoft Dynamics 365 Pro Direct Support, 56
Microsoft Dynamics 365 Enterprise edition - Additional Customer Engagement Social Posts, 56	Microsoft Dynamics AX 2012 R2, 20
Microsoft Dynamics 365 for Customer Service On-premises CAL, 57, 82	Microsoft Dynamics AX 2012 R3 Enterprise Additive CAL, 20
Microsoft Dynamics 365 for Customer Service On-premises CAL, 18	Microsoft Dynamics AX 2012 R3 Enterprise CAL, 20
Microsoft Dynamics 365 for Customer Service, Enterprise edition, 19	Microsoft Dynamics AX 2012 R3 Functional Additive CAL, 20
Microsoft Dynamics 365 for Customer Service, Enterprise Edition (Device SL), 55	Microsoft Dynamics AX 2012 R3 Functional CAL, 20
Microsoft Dynamics 365 for Customer Service, Enterprise edition (User SL), 55	Microsoft Dynamics AX 2012 R3 Self Serve CAL, 20
Microsoft Dynamics 365 for Field Service, Enterprise edition - Resource Scheduling Optimization, 56	Microsoft Dynamics AX 2012 R3 Server, 20
Microsoft Dynamics 365 for Field Service, Enterprise edition (Device SL), 55	Microsoft Dynamics AX 2012 R3 Standard Commerce Server Core, 20
Microsoft Dynamics 365 for Field Service, Enterprise edition (User SL), 55	Microsoft Dynamics AX 2012 R3 Store Server, 20
Microsoft Dynamics 365 for Operations, Enterprise edition, 20, 55	Microsoft Dynamics AX 2012 R3 Task Additive CAL, 20
Microsoft Dynamics 365 for Operations, Enterprise edition - Additional Database Storage, 56	Microsoft Dynamics AX 2012 R3 Task CAL, 20
Microsoft Dynamics 365 for Operations, Enterprise edition - Additional File Storage, 56	Microsoft Dynamics AX Enterprise CAL, 57, 76
Microsoft Dynamics 365 for Operations, Enterprise edition - Sandbox Tier 1	Microsoft Dynamics AX Functional CAL, 57, 76
Developer & Test Instance, 56	Microsoft Dynamics AX Self Serve CAL, 57
	Microsoft Dynamics AX Standard Commerce Core Server, 77
	Microsoft Dynamics AX Store Server, 76

Microsoft Dynamics AX Task CAL, 57, 76
 Microsoft Dynamics CRM 2015, 18
 Microsoft Dynamics CRM 2016, 18
 Microsoft Dynamics CRM Basic CAL, 57
 Microsoft Dynamics CRM Professional CAL, 57
 Microsoft Dynamics CRM Server 2013, 76
 Microsoft Dynamics CRM Server 2015, 76
 Microsoft Exchange Server, 82
 Microsoft Flow Plan 1, 66
 Microsoft Flow Plan 2, 66
 Microsoft Identity Manager 2016 CAL, 21
 Microsoft Identity Manager 2016 External Connector, 21
 Microsoft Intune, 15, 32, 66
 Microsoft Intune Add-on, 66
 Microsoft Intune User SL Add-on Extra Storage 1 GB, 66
 Microsoft Learning E-Reference Library, 66
 Microsoft Learning Imagine Academy, 67
 Microsoft Learning MCP 1 Exam Vouchers, 67
 Microsoft Learning MCP 30 Exam Vouchers, 67
 Microsoft Learning MOS/MCE Certification 125 Exam Site License, 67
 Microsoft Learning MOS/MTA/MCE Certification 500 Exam Site License, 67
 Microsoft Learning MTA/MCA Certification 125 Exam Site License, 67
 Microsoft MultiFactor Authentication, 52
 Microsoft MyAnalytics, 62
 Microsoft Office Audit and Control Management Server 2013, 26
 Microsoft PowerApp Plan 1, 66
 Microsoft PowerApp Plan 2, 66
 Microsoft SQL Server, 82
 Microsoft Translator API, 67
 Minecraft
 Education Edition, 67
 MSDN Platforms, 36
 Office 2013, 22
 Office 2016 for Mac Standard, 23
 Office 365 Advanced Compliance, 62
 Office 365 Advanced Security Management (User SL), 61
 Office 365 Advanced Threat Protection, 62
 Office 365 Business, 57
 Office 365 Business Essentials, 59
 Office 365 Business Premium, 59
 Office 365 Customer Lockbox, 61
 Office 365 Education, 59
 Office 365 Education E5, 59
 Office 365 Education E5 Add-on, 59
 Office 365 Enterprise, 54
 Office 365 Enterprise, 54
 Office 365 Enterprise E1, 15, 59
 Office 365 Enterprise E1 and Microsoft Intune, 15
 Office 365 Enterprise E1 From SA, 59
 Office 365 Enterprise E1, E3 Add-on, 59
 Office 365 Enterprise E3, 15, 59
 Office 365 Enterprise E3 and Microsoft Intune, 15
 Office 365 Enterprise E3 From SA, 59
 Office 365 Enterprise E3 without ProPlus Add-on, 59
 Office 365 Enterprise E4, 59
 Office 365 Enterprise E4 Add-on, 59
 Office 365 Enterprise E4 From SA, 59
 Office 365 Enterprise E4 without ProPlus Add-on, 59
 Office 365 Enterprise E5, 15
 Office 365 Enterprise E5 (User SL), 59
 Office 365 Enterprise E5 Add-on, 59
 Office 365 Enterprise E5 and Microsoft Intune, 15
 Office 365 Enterprise E5 From SA, 59
 Office 365 Enterprise K1, 59
 Office 365 Extra File Storage 1 GB, 64
 Office 365 Midsize Business, 59, 61
 Office 365 Midsize Business Add-on, 60
 Office 365 Pro Plus, 78
 Office 365 ProPlus, 57
 Office 365 ProPlus From SA, 57
 Office for Mac 2011, 23
 Office for Mac Standard, 76
 Office Home & Student 2013 RT Commercial Use, 22
 Office Multi Language Pack, 58, 61
 Office Multi Language Pack 2013, 22
 Office Online, 58
 Office Online for Office 365, 76
 Office Professional Plus, 58, 60, 76, 82
 Office Professional Plus 2013, 58
 Office Professional Plus 2016, 22, 37, 59
 Office Standard, 58, 76, 82
 Office Standard 2016, 22
 OneDrive for Business Plan 1, 63
 OneDrive for Business Plan 2, 63
 Operations Management and Security
 Automation and Control, 52
 Backup and Disaster Recovery, 52
 Insights and Analytics, 52
 Security and Compliance, 52
 Operations Management and Security E1, 52
 Operations Management and Security E1 Add-on, 52
 Operations Management and Security E1 From SA, 52
 Operations Management and Security E2, 52
 Operations Management and Security E2 Add-on, 52
 Operations Management and Security E2 From SA, 52
 Outlook 2016, 22
 Outlook 2016 for Mac, 23
 Power BI Pro, 66
 Power BI Pro A, 66
 PowerPoint 2016, 22
 PowerPoint 2016 for Mac, 23
 Project 2013, 25
 Project Online Essentials, 63
 Project Online Essentials Add-on, 63
 Project Online Premium, 63
 Project Online Premium Add-on, 63
 Project Online Premium From SA, 63
 Project Online Professional, 63
 Project Online Professional Add-on, 63
 Project Online Professional From SA, 63
 Project Professional, 83
 Project Professional 2016, 22

Project Server 2016, 22, 25
 Project Server 2016 CAL, 25
 Project Server 2016 Device CAL, 22
 Project Standard, 76, 83
 Project Standard 2016, 22
 Publisher 2016, 22
 R Server 2016 for Hadoop, 28
 R Server 2016 for Linux, 28
 R Server 2016 for Teradata DB, 28
 Secure Productive Enterprise E3, 53
 Secure Productive Enterprise E3 Add-on, 53
 Secure Productive Enterprise E3 From SA, 53
 Secure Productive Enterprise E5, 53
 Secure Productive Enterprise E5 Add-on, 53
 Secure Productive Enterprise E5 From SA, 53
 SharePoint Online, 76
 SharePoint Online Plan 1, 64
 SharePoint Online Plan 1 Add-on, 64
 SharePoint Online Plan 1 or 2, 26
 SharePoint Online Plan 2, 26, 64
 SharePoint Server, 53, 81
 SharePoint Server 2013, 26
 SharePoint Server 2016, 26
 SharePoint Server 2016 Enterprise CAL, 26
 SharePoint Server 2016 Standard CAL, 26
 Skype for Business 2016, 22
 Skype for Business Online Cloud PBX, 65
 Skype for Business Online Plan 1, 27, 64
 Skype for Business Online Plan 1 Add-on, 60, 64
 Skype for Business Online Plan 2, 27, 65
 Skype for Business Online PSTN Calling, 65
 Skype for Business Online PSTN Conferencing, 65
 Skype for Business Plus CAL, 27
 Skype for Business Plus CAL Add-on for Secure Productive Enterprise E3, 53
 Skype for Business PSTN Consumption, 65
 Skype for Business Server, 53
 Skype for Business Server 2015, 27
 Skype for Business Server 2015 Enterprise CAL, 27
 Skype for Business Server 2015 Plus CAL, 27
 Skype for Business Server 2015 Standard CAL, 27
 SQL Parallel Data Warehouse, 77, 83
 SQL Server, 81
 SQL Server 2014, 29
 SQL Server 2016 CAL, 29
 SQL Server 2016 Enterprise, 29
 SQL Server 2016 Enterprise Core, 29
 SQL Server 2016 Enterprise customers, 29
 SQL Server 2016 Standard, 29
 SQL Server 2016 Standard Core, 29
 SQL Server Business Intelligence, 76, 83
 SQL Server Data Center, 77
 SQL Server Enterprise, 76, 83
 SQL Server Standard, 76, 83
 System Center, 82
 System Center 2012 Client Management Suite, 32, 34, 35
 System Center 2012 Datacenter Server Management License, 77

System Center 2012 R2, 30
 System Center 2012 R2 Configuration Manager, 31
 System Center 2012 R2 Endpoint Protection, 33
 System Center 2012 Standard Server Management License, 76
 System Center 2016 Data Protection Manager, 32
 System Center 2016 Datacenter Server Management License, 30
 System Center 2016 Operations Manager, 34
 System Center 2016 Orchestrator, 34
 System Center 2016 Service Manager, 35
 System Center 2016 Standard Server Management License, 30
 System Center Configuration Manager 1606 Client Management License, 31
 System Center Datacenter, 81, 83
 System Center Datacenter (2-pack Core License), 17
 System Center Endpoint Protection 1606, 33
 System Center Global Service Monitor, 31
 System Center Standard, 81, 83
 System Center Standard (2-pack Core License), 17
 VDI, 36
 Visio 2016 Professional, 22
 Visio 2016 Standard, 22
 Visio Pro for Office 365, 57
 Visio Pro for Office 365 Add-on, 57
 Visio Pro for Office 365 From SA, 57
 Visio Professional, 58, 83
 Visio Standard, 58, 76, 83
 Visual Studio 2013, 36
 Visual Studio Enterprise 2015 with MSDN, 36
 Visual Studio Enterprise with MSDN, 76, 83
 Visual Studio Professional 2015, 36
 Visual Studio Professional 2015 with MSDN, 36
 Visual Studio Professional with MSDN, 76, 83
 Visual Studio Team Foundation Server 2017 CAL, 38
 Visual Studio Team Foundation Server 2017 with SQL Server 2016 Technology, 38
 Visual Studio Test Professional 2015 with MSDN, 36
 Visual Studio Test Professional with MSDN, 76, 83
 Windows 10 Education E5 (Per Device), 39
 Windows 10 Education E5 Per Device Add-on (to E3 per device), 39
 Windows 10 Education Upgrade (Per Device), 39
 Windows 10 Enterprise, 54
 Windows 10 Enterprise E3 and LTSB 2016 Upgrade (Per Device), 39
 Windows 10 Enterprise E3 Per User, 39
 Windows 10 Enterprise E3 Per User Add-on (to E3 per device), 39
 Windows 10 Enterprise E3 Per User From SA, 39
 Windows 10 Enterprise E5 Per Device or User, 39
 Windows 10 Enterprise E5 Per Device or User Add-on (to E3 per device) (SL), 39
 Windows 10 Enterprise E5 Per User From SA, 39
 Windows 10 Enterprise LTSB, 39
 Windows 10 Enterprise LTSB 2016 Upgrade (Per Device), 39
 Windows 10 IoT Enterprise, 40
 Windows 10 IoT Enterprise for Retail or Thin Clients, 40
 Windows 10 Mobile Enterprise (Per Device), 39
 Windows 10 Pro Upgrade, 39
 Windows 2000 Professional for Embedded Systems, 40
 Windows 7, 40

Windows 7 Professional for Embedded Systems, Ultimate for Embedded Systems, 40

Windows 8.1 Enterprise Sideload, 39

Windows Companion Subscription, 42

Windows Embedded 2009, 41

Windows Embedded 8 and 8.1 Industry Retail, 40

Windows Embedded 8 Standard, 41

Windows Embedded 8 Standard Enterprise Kit (100 Pack), 39

Windows Embedded 8.1 Industry, 39

Windows Embedded 8/8.1 Pro, Industry Pro, 40

Windows Embedded for Point of Service, 40

Windows Embedded POSReady 2009, 40

Windows Embedded POSReady 7, 41

Windows Embedded POSReady 7 Pro, 40

Windows Embedded Standard 7, 41

Windows HPC Server, 48

Windows MultiPoint Server 2012, 45

Windows MultiPoint Server 2016 Premium, 45

Windows Server, 82, 83

Windows Server 2012, 46

Windows Server 2012 R2, 46

Windows Server 2016 Active Directory Rights Management Services CAL, 45, 46

Windows Server 2016 Active Directory Rights Management Services External Connector, 46

Windows Server 2016 CAL, 45, 46

Windows Server 2016 Datacenter (2-pack Core License), 46

Windows Server 2016 Essentials, 46

Windows Server 2016 External Connector, 46

Windows Server 2016 Remote Desktop Services CAL, 46

Windows Server 2016 Remote Desktop Services External Connector, 46

Windows Server 2016 Standard (2-pack Core License), 46

Windows Server Datacenter, 77, 81, 83

Windows Server Datacenter (2-pack Core License), 17

Windows Server Enterprise, 48, 76

Windows Server for Itanium Based Systems, 48

Windows Server HPC Edition, 48

Windows Server Standard, 76, 81, 83

Windows Server Standard (2-pack Core License), 17

Windows Small Business Server, 48

Windows Virtual Desktop Access, 39

Windows Vista, 40

Windows Vista Business for Embedded Systems, Ultimate for Embedded Systems, 40

Windows XP, 40

Windows XP Embedded, 41

Windows XP Professional for Embedded Systems, 40

Word 2016, 22

Word 2016 for Mac, 23

Work at Home for Mac 2016, 23

Work at Home for Office Professional Plus 2016, 22

Work at Home for Office Standard 2016, 22

Service Level Agreement for Microsoft Online Services January 1, 2017

Table of Contents

TABLE OF CONTENTS	2	
INTRODUCTION	4	
GENERAL TERMS	5	
SERVICE SPECIFIC TERMS	7	
MICROSOFT DYNAMICS 365	7	
MICROSOFT DYNAMICS 365 FOR CUSTOMER SERVICE	7	
MICROSOFT DYNAMICS 365 FOR FINANCIALS	7	
MICROSOFT DYNAMICS 365 FOR OPERATIONS	7	
MICROSOFT DYNAMICS 365 FOR SALES	8	
OFFICE 365 SERVICES	8	
DUET ENTERPRISE ONLINE	8	
EXCHANGE ONLINE	9	
EXCHANGE ONLINE ARCHIVING	9	
EXCHANGE ONLINE PROTECTION	10	
MICROSOFT TEAMS	10	
MICROSOFT MYANALYTICS	10	
OFFICE 365 BUSINESS	11	
OFFICE 365 CUSTOMER LOCKBOX	11	
OFFICE 365 PROPLUS	11	
OFFICE ONLINE	12	
OFFICE 365 VIDEO	12	
ONEDRIVE FOR BUSINESS	12	
PROJECT ONLINE	13	
SHAREPOINT ONLINE	13	
SKYPE FOR BUSINESS ONLINE	14	
SKYPE FOR BUSINESS ONLINE – PSTN CALLING AND PSTN CONFERENCING	14	
SKYPE FOR BUSINESS ONLINE – VOICE QUALITY	14	
YAMMER ENTERPRISE	15	
MICROSOFT AZURE SERVICES	15	
AD DOMAIN SERVICES	15	
API MANAGEMENT SERVICES	16	
APP SERVICE	16	
APPLICATION INSIGHTS	17	
APPLICATION GATEWAY	17	
AUTOMATION SERVICE – DESIRED STATE CONFIGURATION (DSC)	18	
AUTOMATION SERVICE – PROCESS AUTOMATION	18	
AZURE FUNCTIONS	18	
AZURE SECURITY CENTER	19	
BATCH SERVICE	19	
BACKUP SERVICE	20	
BIZTALK SERVICES	20	
CACHE SERVICES	21	
CDN SERVICE	21	
CLOUD SERVICES	22	
DATA CATALOG	22	
DATA FACTORY – ACTIVITY RUNS	23	
DATA FACTORY – API CALLS	23	
DATA LAKE ANALYTICS	24	
DATA LAKE STORE	24	
DOCUMENTDB	24	
EXPRESSROUTE	25	
HDINSIGHT	25	
HOCKEYAPP	26	
IOT HUB	26	
KEY VAULT	27	
LOG ANALYTICS	27	
LOGIC APPS	27	
MACHINE LEARNING – BATCH EXECUTION SERVICE (BES) AND MANAGEMENT APIS SERVICE	28	
MACHINE LEARNING – REQUEST RESPONSE SERVICE (RRS)	28	
MEDIA SERVICES – CONTENT PROTECTION SERVICE	29	
MEDIA SERVICES – ENCODING SERVICE	29	
MEDIA SERVICES – INDEXER SERVICE	29	
MEDIA SERVICES – LIVE CHANNELS	30	
MEDIA SERVICES – STREAMING SERVICE	30	
MOBILE ENGAGEMENT	31	
MICROSOFT COGNITIVE SERVICES	31	
MOBILE SERVICES	32	
REMOTEAPP	32	
SAP HANA ON AZURE	33	
SCHEDULER	33	
SEARCH	33	
SERVICE-BUS SERVICE – EVENT HUBS	34	
SERVICE-BUS SERVICE – NOTIFICATION HUBS	34	
SERVICE-BUS SERVICE – QUEUES AND TOPICS	35	
SERVICE-BUS SERVICE – RELAYS	35	
SQL DATA WAREHOUSE DATABASE	36	
SQL DATABASE SERVICE (BASIC, STANDARD AND PREMIUM TIERS)	36	
SQL DATABASE SERVICE (WEB AND BUSINESS TIERS)	37	
SQL SERVER STRETCH DATABASE	37	
STORAGE SERVICE	37	
STREAM ANALYTICS – API CALLS	39	
STREAM ANALYTICS – JOBS	39	
TRAFFIC MANAGER SERVICE	40	
VIRTUAL MACHINES	40	
VPN GATEWAY	41	
VISUAL STUDIO ONLINE – BUILD SERVICE	43	
VISUAL STUDIO ONLINE – LOAD TESTING SERVICE	43	
VISUAL STUDIO ONLINE – USER PLANS SERVICE	43	
MICROSOFT AZURE SERVICES PLANS	44	
AZURE ACTIVE DIRECTORY BASIC	44	
AZURE ACTIVE DIRECTORY B2C	44	
AZURE ACTIVE DIRECTORY PREMIUM	45	
AZURE INFORMATION PROTECTION PREMIUM	45	
MICROSOFT CLOUD APP SECURITY	45	
MULTI-FACTOR AUTHENTICATION SERVICE	46	
AZURE SITE RECOVERY SERVICE – ON-PREMISES-TO-AZURE	46	
AZURE SITE RECOVERY SERVICE – ON-PREMISES-TO-ON-PREMISES	47	
STORSIMPLE SERVICE	47	
OTHER ONLINE SERVICES	48	
BING MAPS ENTERPRISE PLATFORM	48	
BING MAPS MOBILE ASSET MANAGEMENT	48	
MICROSOFT FLOW	49	
MICROSOFT INTUNE	49	
MICROSOFT POWERAPPS	50	

MINECRAFT: EDUCATION EDITION 50

POWER BI EMBEDDED 50

POWER BI PRO 51

TRANSLATOR API 51

WINDOWS DESKTOP OPERATING SYSTEM 52

**APPENDIX A – SERVICE LEVEL COMMITMENT FOR VIRUS
DETECTION AND BLOCKING, SPAM EFFECTIVENESS, OR FALSE
POSITIVE 53**

**APPENDIX B - SERVICE LEVEL COMMITMENT FOR UPTIME AND
EMAIL DELIVERY 55**

Introduction

About this Document

This Service Level Agreement for Microsoft Online Services (this “SLA”) is a part of your Microsoft volume licensing agreement (the “Agreement”). Capitalized terms used but not defined in this SLA will have the meaning assigned to them in the Agreement. This SLA applies to the Microsoft Online Services listed herein (a “Service” or the “Services”), but does not apply to separately branded services made available with or connected to the Services or to any on-premise software that is part of any Service.

If we do not achieve and maintain the Service Levels for each Service as described in this SLA, then you may be eligible for a credit towards a portion of your monthly service fees. We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, the version of this SLA that is current at the time of renewal will apply throughout your renewal term. We will provide at least 90 days’ notice for adverse material changes to this SLA. You can review the most current version of this SLA at any time by visiting <http://www.microsoftvolumelicensing.com/SLA>.

Prior Versions of this Document

This SLA provides information on Services currently available. Earlier versions of this document are available at <http://www.microsoftvolumelicensing.com>. To find the needed version, a customer may contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes to this Document

Below are recent additions, deletions and other changes to this SLA. Also listed below, are clarifications of Microsoft policy in response to common customer questions.

Additions	Deletions
Microsoft MyAnalytics	
Microsoft Cognitive Services	

Table of Contents / Definitions

General Terms

Definitions

"Applicable Monthly Period" means, for a calendar month in which a Service Credit is owed, the number of days that you are a subscriber for a Service.

"Applicable Monthly Service Fees" means the total fees actually paid by you for a Service that are applied to the month in which a Service Credit is owed.

"Downtime" is defined for each Service in the Services Specific Terms below. Except for Microsoft Azure Services, Downtime does not include Scheduled Downtime. Downtime does not include unavailability of a Service due to limitations described below and in the Services Specific Terms.

"Error Code" means an indication that an operation has failed, such as an HTTP status code in the 5xx range.

"External Connectivity" is bi-directional network traffic over supported protocols such as HTTP and HTTPS that can be sent and received from a public IP address.

"Incident" means (i) any single event, or (ii) any set of events, that result in Downtime.

"Management Portal" means the web interface, provided by Microsoft, through which customers may manage the Service.

"Scheduled Downtime" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

"Service Credit" is the percentage of the Applicable Monthly Service Fees credited to you following Microsoft's claim approval.

"Service Level" means the performance metric(s) set forth in this SLA that Microsoft agrees to meet in the delivery of the Services.

"Service Resource" means an individual resource available for use within a Service.

"Success Code" means an indication that an operation has succeeded, such as an HTTP status code in the 2xx range.

"Support Window" refers to the period of time during which a Service feature or compatibility with a separate product or service is supported.

"User Minutes" means the total number of minutes in a month, less all Scheduled Downtime, multiplied by the total number of users.

Terms

Claims

In order for Microsoft to consider a claim, you must submit the claim to customer support at Microsoft Corporation including all information necessary for Microsoft to validate the claim, including but not limited to: (i) a detailed description of the Incident; (ii) information regarding the time and duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence.

For a claim related to Microsoft Azure, we must receive the claim within two months of the end of the billing month in which the Incident that is the subject of the claim occurred. For claims related to all other Services, we must receive the claim by the end of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 15th, we must receive the claim and all required information by March 31st.

We will evaluate all information reasonably available to us and make a good faith determination of whether a Service Credit is owed. We will use commercially reasonable efforts to process claims during the subsequent month and within forty-five (45) days of receipt. You must be in compliance with the Agreement in order to be eligible for a Service Credit. If we determine that a Service Credit is owed to you, we will apply the Service Credit to your Applicable Monthly Service Fees.

If you purchased more than one Service (not as a suite), then you may submit claims pursuant to the process described above as if each Service were covered by an individual SLA. For example, if you purchased both Exchange Online and SharePoint Online (not as part of a suite), and during the term of the subscription an Incident caused Downtime for both Services, then you could be eligible for two separate Service Credits (one for each Service), by submitting two claims under this SLA. In the event that more than one Service Level for a particular Service is not met because of the same Incident, you must choose only one Service Level under which to make a claim based on the Incident.

Service Credits

Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA. You may not unilaterally offset your Applicable Monthly Service Fees for any performance or availability issues.

Service Credits apply only to fees paid for the particular Service, Service Resource, or Service tier for which a Service Level has not been met. In cases where Service Levels apply to individual Service Resources or to separate Service tiers, Service Credits apply only to fees paid for the affected

Service Resource or Service tier, as applicable. The Service Credits awarded in any billing month for a particular Service or Service Resource will not, under any circumstance, exceed your monthly service fees for that Service or Service Resource, as applicable, in the billing month. If you purchased Services as part of a suite or other single offer, the Applicable Monthly Service Fees and Service Credit for each Service will be pro-rated.

If you purchased a Service from a reseller, you will receive a service credit directly from your reseller and the reseller will receive a Service Credit directly from us. The Service Credit will be based on the estimated retail price for the applicable Service, as determined by us in our reasonable discretion.

Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center);
2. That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
3. Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised;
4. During or with respect to preview, pre-release, beta or trial versions of a Service, feature or software (as determined by us) or to purchases made using Microsoft subscription credits;
5. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
6. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
7. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
8. That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behavior;
9. Due to your use of Service features that are outside of associated Support Windows; or
10. For licenses reserved, but not paid for, at the time of the Incident.

Services purchased through Open, Open Value, and Open Value Subscription volume licensing agreements, and Services in an Office 365 Small Business Premium suite purchased in the form of a product key are not eligible for Service Credits based on service fees. For these Services, any Service Credit that you may be eligible for will be credited in the form of service time (i.e., days) as opposed to service fees, and any references to "Applicable Monthly Service Fees" is deleted and replaced by "Applicable Monthly Period."

[Table of Contents](#) / [Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Specific Terms

Microsoft Dynamics 365

Microsoft Dynamics 365 for Customer Service

Downtime: Any period of time when end users are unable to read or write any Service data for which they have appropriate permission but this does not include non-availability of Service add-on features.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft Dynamics 365 for Financials

Downtime: Any period of time when end users are unable to login to their instance.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft Dynamics 365 for Operations

Additional Definitions:

"Active Tenant" means a tenant with an active high availability production topology in the Management Portal that (A) has been deployed to a Partner Application Service; and (B) has an active database that users can log into.

"Partner Application Service" means a partner application built on top of and combined with the Platform that (A) is used for processing your organization's actual business transactions; and (B) has reserve compute and storage resources equal to or greater than one of the Scale Units your partner selected for the applicable partner application.

"Maximum Available Minutes" means the total accumulated minutes during a billing month in which an Active Tenant was deployed in a Partner Application Service using an active high availability production topology.

"Platform" means the Service's client forms, SQL server reports, batched operations, and API endpoints, or the Service's retail APIs that are used for commerce or retail purposes only.

"Scale Unit" means the increments by which compute and storage resources are added to or removed from a Partner Application Service.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

“Service Infrastructure” means the authentication, computing, and storage resources that Microsoft provides in connection with the Service.

Downtime: Any period of time when end users are unable to login to their Active Tenant, due to a failure in the unexpired Platform or the Service Infrastructure as Microsoft determines from automated health monitoring and system logs. Downtime does not include Scheduled Downtime, the unavailability of Service add-on features, the inability to access the Service due to your modifications of the Service, or periods where the Scale Unit capacity is exceeded.

Monthly Uptime Percentage: The Monthly Uptime Percentage for a given Active Tenant in a calendar month is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.5%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft Dynamics 365 for Sales

Downtime: Any period of time when end users are unable to read or write any Service data for which they have appropriate permission but this does not include non-availability of Service add-on features.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office 365 Services

Duet Enterprise Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply when the inability to read or write any portion of a SharePoint Online site is caused by any failure of third party software, equipment, or services that are not controlled by Microsoft, or Microsoft software that is not being run by Microsoft itself as part of the Service.

Additional Terms: You will be eligible for a Service Credit for Duet Enterprise Online only when you are eligible for a Service Credit for the SharePoint Online Plan 2 User SLs that you have purchased as a prerequisite for your Duet Enterprise Online User SLs.

[Table of Contents / Definitions](#)

Exchange Online

Downtime: Any period of time when users are unable to send or receive email with Outlook Web Access. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Additional Terms: See Appendix 1 – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive.

[Table of Contents / Definitions](#)

Exchange Online Archiving

Downtime: Any period of time when users are unable to access the email messages stored in their archive. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to the Enterprise CAL suite purchased through Open Value and Open Value Subscription volume licensing agreements.

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

[Table of Contents / Definitions](#)

Exchange Online Protection

Downtime: Any period of time when the network is not able to receive and process email messages. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to the Enterprise CAL suite purchased through Open Value and Open Value Subscription volume licensing agreements.

Additional Terms: See (i) Appendix 1 – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive and (ii) Appendix 2 – Service Level Commitment for Uptime and Email Delivery.

[Table of Contents / Definitions](#)

Microsoft Teams

Downtime: Any period of time when end users are unable to read or post to chat conversations for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft MyAnalytics

Downtime: Any period of time when users are unable to access the MyAnalytics dashboard.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office 365 Business

Downtime: Any period of time when Office applications are put into reduced functionality mode due to an issue with Office 365 activation.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office 365 Customer Lockbox

Downtime: Any period of time when Customer Lockbox is put into reduced functionality mode due to an issue with Office 365.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office 365 ProPlus

Downtime: Any period of time when Office applications are put into reduced functionality mode due to an issue with Office 365 activation.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office Online

Downtime: Any period of time when users are unable to use the Web Applications to view and edit any Office document stored on a SharePoint Online site for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Office 365 Video

Downtime: Any period of time when users are unable to upload, view or edit videos in the video portal when they have appropriate permissions and valid content.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Level Commitment:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

OneDrive for Business

Downtime: Any period of time when users are unable to view or edit files stored on their personal OneDrive for Business storage.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

[Table of Contents](#)

→

[Introduction](#)

→

[General Terms](#)

→

[Service Specific Terms](#)

→

[Appendices](#)

$$\frac{User\ Minutes - Downtime}{User\ Minutes} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Project Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection with Project Web App for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes - Downtime}{User\ Minutes} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

SharePoint Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes - Downtime}{User\ Minutes} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Skype for Business Online

Downtime: Any period of time when end users are unable to see presence status, conduct instant messaging conversations, or initiate online meetings.¹

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

¹Online meeting functionality applicable only to Skype for Business Online Plan 2 Service.

[Table of Contents / Definitions](#)

Skype for Business Online – PSTN Calling and PSTN Conferencing

Downtime: Any period of time when end users are unable to initiate a PSTN call or unable to dial into a PSTN conference.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

Where Downtime is measured in user-minutes; that is, for each month Downtime is the sum of the length (in minutes) of each incident that occurs during that month multiplied by the number of users impacted by that incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Skype for Business Online – Voice Quality

This SLA applies to any eligible call placed by any voice service user within the subscription (enabled for making any type of call VOIP or PSTN).

Additional Definitions:

“Eligible Call” is a Skype for Business placed call (within a subscription) that meets both conditions below:

- The call was placed from a Skype for Business Certified IP Desk phones on wired Ethernet
- Packet Loss, Jitter and Latency issues on the call were due to networks managed by Microsoft.

“Total Calls” is the total number of Eligible Calls

“Poor Quality Calls” is the total number of Eligible Calls that are classified as poor based on numerous factors that could impact call quality in the networks managed by Microsoft. While the current Poor Call classifier is built primarily on network parameters like RTT (Roundtrip Time), Packet Loss Rate, Jitter and Packet Loss-Delay Concealment Factors, it is dynamic and continually updated based on new learnings from analysis using millions of Skype and Skype for Business calls and evolution of Devices, Algorithms and end user ratings.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Monthly Good Call Rate: The Monthly Good Call Rate is calculated using the following formula:

$$\frac{\text{Total Calls} - \text{Poor Quality Calls}}{\text{Total Calls}} \times 100$$

Service Credit:

Monthly Good Call Rate	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Yammer Enterprise

Downtime: Any period of time greater than ten minutes when more than five percent of end users are unable to post or read messages on any portion of the Yammer network for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#) / [Definitions](#)

Microsoft Azure Services

AD Domain Services

Additional Definitions:

"Managed Domain" refers to an Active Directory domain that is provisioned and managed by Azure Active Directory Domain Services.

"Maximum Available Minutes" is the total number of minutes that a given Managed Domain has been deployed by Customer in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

"Downtime" is the total accumulated minutes during a billing month for a given Microsoft Azure subscription during which a given Managed Domain is unavailable. A minute is considered unavailable if all requests for domain authentication of user accounts belonging to the Managed Domain, LDAP bind to the root DSE, or DNS lookup of records, made from within the virtual network where the Managed Domain is enabled, either return an Error Code or fail to return a Success Code within 30 seconds.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Levels and Service Credits are applicable to Customer's use of Azure Active Directory Domain Services:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

API Management Services

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given API Management instance has been deployed in Microsoft Azure during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all API Management instances deployed by you in a given Microsoft Azure subscription during a billing month.

“Proxy” is the component of the API Management Service responsible for receiving API requests and forwarding them to the configured dependent API.

Downtime: The total accumulated Deployment Minutes, across all API Management instances deployed by you in a given Microsoft Azure subscription, during which the API Management Service is unavailable. A minute is considered unavailable for a given API Management instance if all continuous attempts to perform operations through the Proxy throughout the minute result in either an Error Code or do not return a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit for Standard Tier:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Credit for Premium Tier deployments scaled across two or more regions:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

App Service

Additional Definitions:

“App” is an API App, Logic App, Web App or Mobile App deployed by Customer within the App Service, excluding web apps in the Free and Shared tiers.

“Deployment Minutes” is the total number of minutes that a given App has been set to running in Microsoft Azure during a billing month. Deployment Minutes is measured from when the App was created or the Customer initiated an action that would result in running the App to the time the Customer initiated an action that would result in stopping or deleting the App.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Apps deployed by Customer in a given Microsoft Azure subscription during a billing month

Downtime: is the total accumulated Deployment Minutes, across all Apps deployed by Customer in a given Microsoft Azure subscription, during which the App is unavailable. A minute is considered unavailable for a given App when there is no connectivity between the App and Microsoft’s Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Additional Terms: Service Credits are applicable only to fees attributable to your use of Web Apps or Mobile Apps and not to fees attributable to other types of apps available through the App Service, which are not covered by this SLA.

[Table of Contents / Definitions](#)

Application Insights

Additional Definitions:

"Application Insights Resource" is the container in Application Insights that collects, processes and stores the data for a single instrumentation key.

"Maximum Available Minutes" is the total number of minutes that Application Insights Resource(s) have been deployed within a Microsoft Azure subscription during a billing month.

"Data Latency" is the number of minutes that data received from the instrumentation in Customer's application is delayed from appearing in Application Insights service where the delay is greater than 2 hours.

"Downtime" is the total accumulated number of minutes that are part of Maximum Available Minutes that experience Data Latency.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Levels and Service Credits:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Application Gateway

Additional Definitions:

"Application Gateway Cloud Service" refers to a collection of one or more Application Gateway instances configured to perform HTTP load balancing services.

"Maximum Available Minutes" is the total accumulated minutes during a billing month during which an Application Gateway Cloud Service comprising two or more medium or larger Application Gateway instances has been deployed in a Microsoft Azure subscription.

Downtime: is the total accumulated Maximum Available Minutes during a billing month for a given Application Gateway Cloud Service during which the Application Gateway Cloud Service is unavailable. A given minute is considered unavailable if all attempts to connect to the Application Gateway Cloud Service throughout the minute are unsuccessful.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

[Table of Contents](#)

→

[Introduction](#)

→

[General Terms](#)

→

[Service Specific Terms](#)

→

[Appendices](#)

Automation Service – Desired State Configuration (DSC)

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Automation account has been deployed in Microsoft Azure during a billing month.

“DSC Agent Service” is the component of the Automation Service responsible for receiving and responding to pull, registration, and reporting requests from DSC nodes.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Automation accounts deployed in a given Microsoft Azure subscription during a billing month

Downtime: The total accumulated Deployment Minutes, across all Automation accounts deployed in a given Microsoft Azure subscription, during which the DSC Agent Service is unavailable. A minute is considered unavailable for a given Automation account if all continuous pull, registration, and reporting requests from DSC nodes associated with the Automation account to the DSC Agent Service throughout the minute either result in an Error Code or do not return a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Automation Service – Process Automation

Additional Definitions:

“Delayed Jobs” is the total number of Jobs, for a given Microsoft Azure subscription, that fail to start within thirty (30) minutes of their Planned Start Times.

“Job” means the execution of a Runbook.

“Planned Start Time” is a time at which a Job is scheduled to begin executing.

“Runbook” means a set of actions specified by you to execute within Microsoft Azure.

“Total Jobs” is the total number of Jobs scheduled for execution during a given billing month, for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Jobs} - \text{Delayed Jobs}}{\text{Total Jobs}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Azure Functions

For Function Apps running on App Service Plans we guarantee that the associated Functions compute will be available 99.95% of the time. No SLA is provided for Functions Apps running under Consumption Plans.

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Function App is available to be triggered during a billing month. Deployment Minutes are measured based on the total time that the service is available to trigger a function execution and not based on the potential number of Function executions that might be triggered during a given month.

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

"Maximum Available Minutes" is the sum of all Deployment Minutes across all Function Apps deployed by Customer in a given Microsoft Azure subscription during a billing month.

"Function App" is an individual Function deployed on an App Service Plan with an associated trigger.

"Downtime" The total accumulated Deployment Minutes, across the Function App deployed by a customer in a given Microsoft Azure subscription, during which the Function App is unavailable to be triggered. A minute is considered unavailable for a given Function App when there is no connectivity between the App Service Plan on which the Function App is hosted and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Azure Security Center

Additional Definitions:

"Protected Node" is a Microsoft Azure resource, counted as a node for billing purposes that is configured for the Azure Security Center Standard Tier

"Security Monitoring" is the assessment of a Protected Node resulting in potential findings such as security health status, recommendations, and security alerts, exposed in Azure Security Center.

"Maximum Available Minutes" is the total number of minutes during a billing month that a given Protected Node has been deployed and configured for Security Monitoring.

"Downtime" is the total accumulated minutes during a billing month for which Security Monitoring information of a given Protected Node is unavailable. A minute is considered unavailable for a given Protected Node if all continuous attempts to retrieve Security Monitoring information throughout the minute result in either an Error Code or do not return a Success Code within two minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Batch Service

Additional Definitions:

"Average Error Rate" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"Error Rate" is the total number of Failed Requests divided by Total Requests during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

"Excluded Requests" are requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"Failed Requests" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 5 seconds.

"Total Requests" is the total number of authenticated REST API requests, other than Excluded Requests, to perform operations against Batch accounts attempted within a one-hour interval within a given Azure subscription during a billing month.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \text{Average Error Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Backup Service

Additional Definitions:

“Backup” or **“Back Up”** is the process of copying computer data from a registered server to a Backup Vault.

“Backup Agent” refers to the software installed on a registered server that enables the registered server to Back Up or Restore one or more Protected Items.

“Backup Vault” refers to a container in which you may register one or more Protected Items for Backup.

“Deployment Minutes” is the total number of minutes during which a Protected Item has been scheduled for Backup to a Backup Vault.

“Failure” means that either the Backup Agent or the Service fails to fully complete a properly configured Backup or Recovery operation due to unavailability of the Backup Service.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Protected Items for a given Microsoft Azure subscription during a billing month.

“Protected Item” refers to a collection of data, such as a volume, database, or virtual machine that has been scheduled for Backup to the Backup Service such that it is enumerated as a Protected Item in the Protected Items tab in the Recovery Services section of the Management Portal.

“Recovery” or **“Restore”** is the process of restoring computer data from a Backup Vault to a registered server.

Downtime: The total accumulated Deployment Minutes across all Protected Items scheduled for Backup by you in a given Microsoft Azure subscription during which the Backup Service is unavailable for the Protected Item. The Backup Service is considered unavailable for a given Protected Item from the first Failure to Back Up or Restore the Protected Item until the initiation of a successful Backup or Recovery of a Protected Item, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

BizTalk Services

Additional Definitions:

“BizTalk Service Environment” refers to a deployment of the BizTalk Services created by you, as represented in the Management Portal, to which you may send runtime message requests.

“Deployment Minutes” is the total number of minutes that a given BizTalk Service Environment has been deployed in Microsoft Azure during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all BizTalk Service Environments deployed by you in a given Microsoft Azure subscription during a billing month.

“Monitoring Storage Account” refers to the Azure Storage account used by the BizTalk Services to store monitoring information related to the execution of the BizTalk Services.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Downtime: The total accumulated Deployment Minutes, across all BizTalk Service Environments deployed by you in a given Microsoft Azure subscription, during which the BizTalk Service Environment is unavailable. A minute is considered unavailable for a given BizTalk Service Environment when there is no connectivity between your BizTalk Service Environment and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic, Standard, and Premium tiers of the BizTalk Services. The Developer tier of the Microsoft Azure BizTalk Services is not covered by this SLA.

Additional Terms: When submitting a claim, you must ensure that complete monitoring data is maintained within the Monitoring Storage Account and is made available to Microsoft.

[Table of Contents / Definitions](#)

Cache Services

Additional Definitions:

"Cache" refers to a deployment of the Cache Service created by you, such that its Cache Endpoints are enumerated in the Cache tab in the Management Portal.

"Cache Endpoints" refers to endpoints through which a Cache may be accessed.

"Deployment Minutes" is the total number of minutes that a given Cache has been deployed in Microsoft Azure during a billing month.

"Maximum Available Minutes" is the sum of all Deployment Minutes across all Caches deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Caches deployed by you in a given Microsoft Azure subscription, during which the Cache is unavailable. A minute is considered unavailable for a given Cache when there is no connectivity throughout the minute between one or more Cache Endpoints associated with the Cache and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Cache Service, which includes the Azure Managed Cache Service or the Standard tier of the Azure Redis Cache Service. The Basic tier of the Azure Redis Cache Service is not covered by this SLA.

[Table of Contents / Definitions](#)

CDN Service

Downtime: To assess Downtime, Microsoft will review data from any commercially reasonable independent measurement system used by you.

You must select a set of agents from the measurement system's list of standard agents that are generally available and represent at least five geographically diverse locations in major worldwide metropolitan areas (excluding PR of China).

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Measurement System tests (frequency of at least one test per hour per agent) will be configured to perform one HTTP GET operation according to the model below:

1. A test file will be placed on your origin (e.g., Azure Storage account).
2. The GET operation will retrieve the file through the CDN Service, by requesting the object from the appropriate Microsoft Azure domain name hostname.
3. The test file will meet the following criteria:
 - i. The test object will allow caching by including explicit "Cache-control: public" headers, or lack of "Cache-Control: private" header.
 - ii. The test object will be a file at least 50KB in size and no larger than 1MB.
 - iii. Raw data will be trimmed to eliminate any measurements that came from an agent experiencing technical problems during the measurement period.

Monthly Uptime Percentage: The percentage of HTTP transactions in which the CDN responds to client requests and delivers the requested content without error. Monthly Uptime Percentage of the CDN Service is calculated as the number of times the object was delivered successfully divided by the total number of requests (after removing erroneous data).

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99.5%	25%

[Table of Contents / Definitions](#)

Cloud Services

Additional Definitions:

"Cloud Services" refers to a set of compute resources utilized for Web and Worker Roles.

"Maximum Available Minutes" is the total accumulated minutes during a billing month for all Internet facing roles that have two or more instances deployed in different Update Domains. Maximum Available Minutes is measured from when the Tenant has been deployed and its associated roles have been started resultant from action initiated by you to the time you have initiated an action that would result in stopping or deleting the Tenant.

"Tenant" represents one or more roles each consisting of one or more role instances that are deployed in a single package.

"Update Domain" refers to a set of Microsoft Azure instances to which platform updates are concurrently applied.

"Web Role" is a Cloud Services component run in the Azure execution environment that is customized for web application programming as supported by IIS and ASP.NET.

"Worker Role" is a Cloud Services component run in the Azure execution environment that is useful for generalized development, and may perform background processing for a Web Role.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes that have no External Connectivity.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Data Catalog

Additional Definitions:

"Deployment Minutes" is the total number of minutes for which a Data Catalog has been purchased during a billing month.

"Entries" means any catalog object registration in the Data Catalog (such as a table, view, measure, cluster or report).

"Maximum Available Minutes" is the sum of all Deployment Minutes for the Data Catalog associated with a given Microsoft Azure subscription during a billing month.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Downtime: is the total accumulated Deployment minutes, during which the Data Catalog is unavailable. A minute is considered unavailable for a given Data Catalog if all attempts by administrators to add or remove users to the Data Catalog or all attempts by users to execute API calls to the Data Catalog for registering, searching, or deleting Entries either result in an Error Code or do not return a response within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Data Factory – Activity Runs

Additional Definitions:

“**Activity Run**” means the execution or attempted execution of an activity

“**Delayed Activity Runs**” is the total number of attempted Activity Runs in which an activity fails to begin executing within four (4) minutes after the time at which it is scheduled for execution and all dependencies that are prerequisite to execution have been satisfied.

“**Total Activity Runs**” is the total number of Activity Runs attempted during in a billing month for a given Microsoft Azure Subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Activity Runs} - \text{Delayed Activity Runs}}{\text{Total Activity Runs}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Data Factory – API Calls

Additional Definitions:

“**Excluded Requests**” is the set of requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

“**Failed Requests**” is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or otherwise fail to return a Success Code within two minutes.

“**Resources**” means pipelines, data sets, and linked services created within a Data Factory.

“**Total Requests**” is the set of all requests, other than Excluded Requests, to perform operations against Resources within active pipelines during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Requests} - \text{Failed Requests}}{\text{Total Requests}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Data Lake Analytics

Additional Definitions:

"Total Operations" is the total number of authenticated operations attempted within a one-hour interval across all Data Lake Analytics accounts in a given Azure subscription during a billing month.

"Failed Operations" is the set of all operations within Total Operations that either return an Error Code or fail to return a Success Code within 5 minutes for account creation and deletion and 25 seconds for all other operations with an additional 2 seconds per MB for operations with payload.

"Error Rate" is the total number of Failed Operations divided by Total Operations during a given one-hour interval. If the Total Operations in a one-hour interval is zero, the Error Rate for that interval is 0%.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \text{Average Error Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Data Lake Store

Additional Definitions:

"Total Operations" is the total number of authenticated operations attempted within a one-hour interval across all Data Lake Store accounts in a given Azure subscription during a billing month.

"Failed Operations" is the set of all operations within Total Operations that either return an Error Code or fail to return a Success Code within 5 minutes for account creation and deletion, 2 seconds per file for operations on multiple files, 2 seconds per MB for data transfer operations, and 2 seconds for all other operations.

"Error Rate" is the total number of Failed Operations divided by Total Operations during a given one-hour interval. If the Total Operations in a one-hour interval is zero, the Error Rate for that interval is 0%.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \text{Average Error Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

DocumentDB

Additional Definitions:

"Average Error Rate" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"Database Account" is a DocumentDB account containing one or more databases.

"Error Rate" is the total number of Failed Requests divided by Total Requests, across all Resources in a given Azure subscription, during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

"Excluded Requests" are requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"Failed Requests" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 5 seconds.

"Resource" is a set of URI addressable entities associated with a Database Account.

"Total Request" is the set of all requests, other than Excluded Requests, to perform operations issued against Resources attempted within a one-hour interval within a given Azure subscription during a billing month.

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \text{Average Error Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

[Table of Contents / Definitions](#)

ExpressRoute

Additional Definitions:

“Dedicated Circuit” means a logical representation of connectivity offered through the ExpressRoute Service between your premises and Microsoft Azure through an exchange provider or a network service provider, where such connectivity does not traverse the public Internet.

“Maximum Available Minutes” is the total number of minutes that a given Dedicated Circuit is linked to one or more Virtual Networks in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

“Virtual Network” refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within Microsoft Azure.

“VPN Gateway” refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

Downtime: The total accumulated minutes during a billing month for a given Microsoft Azure subscription during which the Dedicated Circuit is unavailable. A minute is considered unavailable for a given Dedicated Circuit if all attempts by you within the minute to establish IP-level connectivity to the VPN Gateway associated with the Virtual Network fail for longer than thirty seconds.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Additional Terms: Monthly Uptime Percentage and Service Credits are calculated for each Dedicated Circuit used by you.

[Table of Contents / Definitions](#)

HDInsight

Additional Definitions:

“Cluster Internet Gateway” means a set of virtual machines within an HDInsight Cluster that proxy all connectivity requests to the Cluster.

“Deployment Minutes” is the total number of minutes that a given HDInsight Cluster has been deployed in Microsoft Azure.

“HDInsight Cluster” or **“Cluster”** means a collection of virtual machines running a single instance of the HDInsight Service.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Clusters deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes when the HDInsight Service is unavailable. A minute is considered unavailable for a given Cluster if all continual attempts within the minute to establish a connection to the Cluster Internet Gateway fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

HockeyApp

Additional Definitions:

"HockeyApp Dashboard" means the web interface provided to developers to view and manage applications using the HockeyApp Service.

"Maximum Available Minutes" is the total number of minutes in a billing month.

Downtime: is the total accumulated minutes in a billing month during which the HockeyApp Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the HockeyApp Dashboard or to the HockeyApp API throughout the minute either result in an Error Code or do not return a response within one minute. For purposes of the HockeyApp API, HTTP response codes 408, 429, 500, 503, and 511 are not considered Error Codes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

IoT hub

Additional Definitions:

"Deployment Minutes" is the total number of minutes that a given IoT hub has been deployed in Microsoft Azure during a billing month.

"Device Identity Operations" refers to create, read, update, and delete operations performed on the device identity registry of an IoT hub.

"Maximum Available Minutes" is the sum of all Deployment Minutes across all IoT hubs deployed in a given Microsoft Azure subscription during a billing month.

"Message" refers to any content sent by a deployed IoT hub to a device registered to the IoT hub or received by the IoT hub from a registered device, using any protocol supported by the Service.

Downtime: The total accumulated Deployment Minutes, across all IoT hubs deployed in a given Microsoft Azure subscription, during which the IoT hub is unavailable. A minute is considered unavailable for a given IoT hub if all continuous attempts to send or receive Messages or perform Device Identity Operations on the IoT hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

Key Vault

Additional Definitions:

"Deployment Minutes" is the total number of minutes that a given key vault has been deployed in Microsoft Azure during a billing month.

"Excluded Transactions" are transactions for creating, updating, or deleting key vaults, keys, or secrets.

"Maximum Available Minutes" is the sum of all Deployment Minutes across all Key Vaults deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated Deployment Minutes, across all key vaults deployed by Customer in a given Microsoft Azure subscription, during which the key vault is unavailable. A minute is considered unavailable for a given key vault if all continuous attempts to perform transactions, other than Excluded Transactions, on the key vault throughout the minute either return an Error Code or do not result in a Success Code within 5 seconds from Microsoft's receipt of the request.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Log Analytics

Additional Definitions:

"Batch" means a group of Log Data entries that are either uploaded to the Log Analytics Service or read from storage by the Log Analytics Service within a given period of time. Batches queued for indexing are displayed in the usage section of the Management Portal.

"Log Data" refers to information regarding a supported event, such as IIS and Windows events, that is logged by a computer and for which the Log Analytics Service has been configured to be processed by the Service index.

"Delayed Batches" is the total number of Batches within Total Queued Batches that fail to complete indexing within six hours of the Batch being queued.

"Total Queued Batches" is the total number of Batches queued for indexing by the Log Analytics Service during a given billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Queued Batches} - \text{Delayed Batches}}{\text{Total Queued Batches}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Logic Apps

Additional Definitions:

"Deployment Minutes" is the total number of minutes that a given Logic App has been set to running in Microsoft Azure during a billing month. Deployment Minutes is measured from when the Logic App was created or Customer initiated an action that would result in running the Logic App to the time Customer initiated an action that would result in stopping or deleting the Logic App.

"Maximum Available Minutes" is the sum of all Deployment Minutes across all Logic Apps deployed by Customer in a given Microsoft Azure subscription during a billing month.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

“Downtime” The total accumulated Deployment Minutes, across all Logic Apps deployed by Customer in a given Microsoft Azure subscription, during which the Logic App is unavailable. A minute is considered unavailable for a given Logic App when there is no connectivity between the Logic App and Microsoft’s Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Machine Learning – Batch Execution Service (BES) and Management APIs Service

Additional Definitions:

“Failed Transactions” is the set of all requests within Total Transaction Attempts that return an Error Code.

“Total Transaction Attempts” is the total number of authenticated REST BES and Management API requests by you during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: Service Levels and Service Credits are applicable to your use of the Machine Learning BES and Management API Service. The Free Machine Learning tier is not covered by this SLA.

[Table of Contents / Definitions](#)

Machine Learning – Request Response Service (RRS)

Additional Definitions:

“Failed Transactions” is the set of all requests within Total Transaction Attempts that return an Error Code.

“Total Transaction Attempts” is the total number of authenticated REST RRS and Management API requests by you during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Service Level Exceptions: Service Levels and Service Credits are applicable to your use of the Machine Learning RRS and Management API Service. The Free Machine Learning tier is not covered by this SLA.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

[Table of Contents / Definitions](#)

Media Services – Content Protection Service

Additional Definitions:

“Failed Transactions” are all Valid Key Requests included in Total Transaction Attempts that result in an Error Code or otherwise do not return a Success Code within 30 seconds after receipt by the Content Protection Service.

“Total Transaction Attempts” are all Valid Key Requests made by you during a billing month for a given Azure subscription.

“Valid Key Requests” are all requests made to the Content Protection Service for existing content keys in a Customer's Media Service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Media Services – Encoding Service

Additional Definitions:

“Encoding” means the processing of media files per subscription as configured in the Media Services Tasks.

“Failed Transactions” is the set of all requests within Total Transaction Attempts that do not return a Success Code within 30 seconds from Microsoft's receipt of the request.

“Media Service” means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

“Media Services Task” means an individual operation of media processing work as configured by you. Media processing operations involve encoding and converting media files.

“Total Transaction Attempts” is the total number of authenticated REST API requests with respect to a Media Service made by you during a billing month for a subscription. Total Transaction Attempts does not include REST API requests that return an Error Code that are continuously repeated within a five-minute window after the first Error Code is received.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Media Services – Indexer Service

Additional Definitions:

“Encoding Reserved Unit” means encoding reserved units purchased by the customer in an Azure Media Services account

“Failed Transactions” is the set of Indexer Tasks within Total Transaction Attempts that either, a) do not complete within a time period that is 3 times the duration of the input file, or b) do not start processing within 5 minutes of the time that an Encoding Reserved Unit becomes available for use by the Indexer Task.

“Indexer Task” means a Media Services Task that is configured to index an MP3 input file with a minimum five-minute duration.

“Total Transaction Attempts” is the total number of Indexer Tasks attempted to be executed using an available Encoding Reserved Unit by Customer during a billing month for a subscription.

[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Media Services – Live Channels

Additional Definitions:

“Channel” means an end point within a Media Service that is configured to receive media data.

“Deployment Minutes” is the total number of minutes that a given Channel has been purchased and allocated to a Media Service and is in a running state during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Channels purchased and allocated to a Media Service during a billing month.

“Media Service” means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

Downtime: The total accumulated Deployment Minutes when the Live Channels Service is unavailable. A minute is considered unavailable for a given Channel if the Channel has no External Connectivity during the minute.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Media Services – Streaming Service

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Streaming Unit has been purchased and allocated to a Media Service during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Streaming Units purchased and allocated to a Media Service during a billing month.

“Media Service” means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

“Media Service Request” means a request issued to your Media Service.

“Streaming Unit” means a unit of reserved egress capacity purchased by you for a Media Service.

“Valid Media Services Requests” are all qualifying Media Service Requests for existing media content in a customer’s Azure Storage account associated with its Media Service when at least one Streaming Unit has been purchased and allocated to that Media Service. Valid Media Services Requests do not include Media Service Requests for which total throughput exceeds 80% of the Allocated Bandwidth.

Downtime: The total accumulated Deployment Minutes when the Streaming Service is unavailable. A minute is considered unavailable for a given Streaming Unit if all continuous Valid Media Service Requests made to the Streaming Unit throughout the minute result in an Error Code.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Mobile Engagement

Additional Definitions:

"Average Error Rate" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"Error Rate" is the total number of Failed Requests divided by Total Requests during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

"Excluded Requests" is the set of REST API requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"Failed Requests" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 30 seconds.

"Mobile Engagement Application" is an Azure Mobile Engagement service instance.

"Total Requests" is the total number of authenticated REST API requests, other than Excluded Requests, made to Mobile Engagement Applications within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \text{Average Error Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

The Free Mobile Engagement tier is not covered by this SLA.

[Table of Contents / Definitions](#)

Microsoft Cognitive Services

Additional Definitions:

"Total Transaction Attempts" is the total number of authenticated API requests by Customer during a billing month for a given Cognitive Service API. Total Transaction Attempts do not include API requests that return an Error Code that are continuously repeated within a five-minute window after the first Error Code is received.

"Failed Transactions" is the set of all requests to the Cognitive Service API within Total Transaction Attempts that return an Error Code in 5xx range. Failed Transaction Attempts do not include API requests that return an Error Code that are continuously repeated within a five-minute window after the first Error Code is received.

Monthly Uptime Percentage: for each API Service is calculated as Total Transaction Attempts less Failed Transactions divided by Total Transaction Attempts in a billing month for a given API subscription. Monthly Uptime Percentage is represented by the following formula:

$$\frac{(\text{Total Transaction Attempts} - \text{Failed Transactions})}{\text{Total Transaction Attempts}} \times 100$$

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Credit: The following Service Levels and Service Credits are applicable to APIs running in the Standard tier

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: No SLA is provided to free tier or offerings in preview.

[Table of Contents / Definitions](#)

Mobile Services

Additional Definitions:

“Failed Transactions” include any API calls included in Total Transaction Attempts that result in either an Error Code or do not return a Success Code.

“Total Transaction Attempts” are the total accumulated API calls made to the Azure Mobile Services during a billing month for a given Microsoft Azure subscription for which the Azure Mobile Services are running.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Standard and Premium Mobile Services tiers. The Free Mobile Services tier is not covered by this SLA.

[Table of Contents / Definitions](#)

RemoteApp

Additional Definitions:

“Application” means a software application that is configured for streaming to a device using the RemoteApp Service.

“Maximum Available Minutes” is the sum of all User Application Minutes across all Users granted access to one or more Applications in a given Azure subscription during a billing month.

“User” means a specific user account that is able to stream an Application using the RemoteApp Service, as enumerated in the Management Portal.

“User Application Minutes” is the total number of minutes in a billing month during which you have granted a User access to an Application.

Downtime: The total accumulated User Minutes during which the RemoteApp Service is unavailable. A minute is considered unavailable for a given User when the User is unable to establish connectivity to an Application.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the RemoteApp Service. The RemoteApp free trial is not covered by this SLA.

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

SAP HANA on Azure

Additional Definitions:

"High Availability Pair" refers to two or more identical SAP HANA on Azure large instances deployed in the same region and configured by the customer for system replication at the application layer. Customer must declare the members of a High Availability Pair to Microsoft during the architecture design process.

"SAP HANA on Azure Connectivity" is bi-directional network traffic between the SAP HANA on Azure large instance and other IP addresses using TCP or UDP network protocols in which the instance is configured for allowed traffic. The IP addresses can be IP addresses within the same virtual network as the virtual machine or public, routable IP addresses.

"Maximum Available Minutes" is the total accumulated minutes during a billing month for all SAP HANA on Azure instances deployed in the same High Availability Pair. Maximum Available Minutes is measured from when two or more instances in the same High Availability Pair have both been started resultant from an action initiated by Customer to the time Customer has initiated an action that would result in stopping the instances.

"Downtime" is the total accumulated minutes that are part of Maximum Available Minutes that have no SAP HANA on Azure Connectivity.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99.9%	25%

[Table of Contents / Definitions](#)

Scheduler

Additional Definitions:

"Maximum Available Minutes" is the total number of minutes in a billing month.

"Planned Execution Time" is a time at which a Scheduled Job is scheduled to begin executing.

"Scheduled Job" means an action specified by you to execute within Microsoft Azure according to a specified schedule.

Downtime: The total accumulated minutes in a billing month during which one or more of your Scheduled Jobs is in a state of delayed execution. A given Scheduled Job is in a state of delayed execution if it has not begun executing after a Planned Execution Time, provided that such delayed execution time shall not be considered Downtime if the Scheduled Job begins executing within thirty (30) minutes after a Planned Execution Time.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Search

Additional Definitions:

"Average Error Rate" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"Error Rate" is the total number of Failed Requests divided by Total Requests, across all Search Service Instances in a given Azure subscription, during a given one-hour interval. If the Total Requests in a one-hour interval is zero, the Error Rate for that interval is 0%.

[Table of Contents](#)

→

[Introduction](#)

→

[General Terms](#)

→

[Service Specific Terms](#)

→

[Appendices](#)

“Excluded Requests” are all requests that are throttled due to exhaustion of resources allocated for a Search Service Instance, as indicated by an HTTP 503 status code and a response header indicating the request was throttled.

“Failed Requests” is the set of all requests within Total Requests that fail to return either a Success Code or HTTP 4xx response.

“Replica” is a copy of a search index within a Search Service Instance.

“Search Service Instance” is an Azure Search service instance containing one or more search indexes.

“Total Requests” is the set of (i) all requests to update a Search Service Instance having three or more Replicas, plus (ii) all requests to query a Search Service Instance having two or more Replicas, other than Excluded Requests, within a one-hour interval within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \text{Average Error Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Free Search tier is not covered by this SLA.

[Table of Contents / Definitions](#)

Service-Bus Service – Event Hubs

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Event Hub has been deployed in Microsoft Azure during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Event Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Event Hubs tiers during a billing month.

“Message” refers to any user-defined content sent or received through Service Bus Relays, Queues, Topics, or Notification Hubs, using any protocol supported by Service Bus.

Downtime: The total accumulated Deployment Minutes, across all Event Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Event Hubs tiers, during which the Event Hub is unavailable. A minute is considered unavailable for a given Event Hub if all continuous attempts to send or receive Messages or perform other operations on the Event Hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic and Standard Event Hubs tiers. The Free Event Hubs tier is not covered by this SLA.

[Table of Contents / Definitions](#)

Service-Bus Service – Notification Hubs

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Notification Hub has been deployed in Microsoft Azure during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Notification Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Notification Hubs tiers during a billing month.

[Table of Contents](#)

→

[Introduction](#)

→

[General Terms](#)

→

[Service Specific Terms](#)

→

[Appendices](#)

Downtime: The total accumulated Deployment Minutes, across all Notification Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Notification Hubs tiers, during which the Notification Hub is unavailable. A minute is considered unavailable for a given Notification Hub if all continuous attempts to send notifications or perform registration management operations with respect to the Notification Hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic and Standard Notification Hubs tiers. The Free Notification Hubs tier is not covered by this SLA.

[Table of Contents / Definitions](#)

Service-Bus Service – Queues and Topics

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Queue or Topic has been deployed in Microsoft Azure during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Queues and Topics deployed by you in a given Microsoft Azure subscription during a billing month.

“Message” refers to any user-defined content sent or received through Service Bus Relays, Queues, Topics, or Notification Hubs, using any protocol supported by Service Bus.

Downtime: The total accumulated Deployment Minutes, across all Queues and Topics deployed by you in a given Microsoft Azure subscription, during which the Queue or Topic is unavailable. A minute is considered unavailable for a given Queue or Topic if all continuous attempts to send or receive Messages or perform other operations on the Queue or Topic throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Service-Bus Service – Relays

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Relay has been deployed in Microsoft Azure during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Relays deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Relays deployed by you in a given Microsoft Azure subscription, during which the Relay is unavailable. A minute is considered unavailable for a given Relay if all continuous attempts to establish a connection to the Relay throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

SQL Data Warehouse Database

Additional Definitions:

“Database” means any SQL Data Warehouse Database.

“Maximum Available Minutes” is the total number of minutes that a given Database has been deployed in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

“Client Operations” is the set of all documented operations supported by SQL Data Warehouse.

Downtime: is the total accumulated minutes during a billing month for a given Microsoft Azure subscription during which a given Database is unavailable. A minute is considered unavailable for a given Database if more than 1% of all Client Operations completed during the minute return an Error Code.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

SQL Database Service (Basic, Standard and Premium Tiers)

Additional Definitions:

“Database” means any single or elastic Basic, Standard, or Premium Microsoft Azure SQL Database.

“Maximum Available Minutes” is the total number of minutes that a given Database has been deployed in in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

Downtime: is the total accumulated minutes during a billing month for a given Microsoft Azure subscription during which a given Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

[Table of Contents / Definitions](#)
[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

SQL Database Service (Web and Business Tiers)

Additional Definitions:

"Database" means any Web or Business Microsoft Azure SQL Database.

"Deployment Minutes" is the total number of minutes that a given Web or Business Database has been deployed in Microsoft Azure during a billing month.

"Maximum Available Minutes" is the sum of all Deployment Minutes across all Web and Business Databases for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes across all Web and Business Databases deployed by you in a given Microsoft Azure subscription during which the Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts by you to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

SQL Server Stretch Database

Additional Definitions:

"Database" means one instance of SQL Server Stretch Database.

"Maximum Available Minutes" is the total number of minutes that a given Database has been deployed in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated minutes across all Databases deployed by Customer in a given Microsoft Azure subscription during which the Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts by Customer to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Storage Service

Additional Definitions:

"Average Error Rate" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"Blob Storage Account" is a storage account specialized for storing data as blobs and provides the ability to specify an access tier indicating how frequently the data in that account is accessed.

"Cool Access Tier" is an attribute of a Blob Storage Account indicating that the data in the account is infrequently accessed and has a lower availability service level than data in other access tiers.

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

“Excluded Transactions” are storage transactions that do not count toward either Total Storage Transactions or Failed Storage Transactions. Excluded Transactions include pre-authentication failures; authentication failures; attempted transactions for storage accounts over their prescribed quotas; creation or deletion of containers, tables, or queues; clearing of queues; and copying blobs between storage accounts.

“Error Rate” is the total number of Failed Storage Transactions divided by the Total Storage Transactions during a set time interval (currently set at one hour). If the Total Storage Transactions in a given one-hour interval is zero, the error rate for that interval is 0%.

“Failed Storage Transactions” is the set of all storage transactions within Total Storage Transactions that are not completed within the Maximum Processing Time associated with their respective transaction type, as specified in the table below. Maximum Processing Time includes only the time spent processing a transaction request within the Storage Service and does not include any time spent transferring the request to or from the Storage Service.

Request Types	Maximum Processing Time
PutBlob and GetBlob (includes blocks and pages) Get Valid Page Blob Ranges	Two (2) seconds multiplied by the number of MBs transferred in the course of processing the request
Copy Blob	Ninety (90) seconds (where the source and destination blobs are within the same storage account)
PutBlockList GetBlockList	Sixty (60) seconds
Table Query List Operations	Ten (10) seconds (to complete processing or return a continuation)
Batch Table Operations	Thirty (30) seconds
All Single Entity Table Operations All other Blob and Message Operations	Two (2) seconds

These figures represent maximum processing times. Actual and average times are expected to be much lower.

Failed Storage Transactions do not include:

1. Transaction requests that are throttled by the Storage Service due to a failure to obey appropriate back-off principles.
2. Transaction requests having timeouts set lower than the respective Maximum Processing Times specified above.
3. Read transactions requests to RA-GRS Accounts for which you did not attempt to execute the request against Secondary Region associated with the storage account if the request to the Primary Region was not successful.
4. Read transaction requests to RA-GRS Accounts that fail due to Geo-Replication Lag.

“Geo Replication Lag” for GRS and RA-GRS Accounts is the time it takes for data stored in the Primary Region of the storage account to replicate to the Secondary Region of the storage account. Because GRS and RA-GRS Accounts are replicated asynchronously to the Secondary Region, data written to the Primary Region of the storage account will not be immediately available in the Secondary Region. You can query the Geo Replication Lag for a storage account, but Microsoft does not provide any guarantees as to the length of any Geo Replication Lag under this SLA.

“Geographically Redundant Storage (GRS) Account” is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You cannot directly read data from or write data to the Secondary Region associated with GRS Accounts.

“Locally Redundant Storage (LRS) Account” is a storage account for which data is replicated synchronously only within a Primary Region.

“Primary Region” is a geographical region in which data within a storage account is located, as selected by you when creating the storage account. You may execute write requests only against data stored within the Primary Region associated with storage accounts.

“Read Access Geographically Redundant Storage (RA-GRS) Account” is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You can directly read data from, but cannot write data to, the Secondary Region associated with RA-GRS Accounts.

“Secondary Region” is a geographical region in which data within a GRS or RA-GRS Account is replicated and stored, as assigned by Microsoft Azure based on the Primary Region associated with the storage account. You cannot specify the Secondary Region associated with storage accounts.

“Total Storage Transactions” is the set of all storage transactions, other than Excluded Transactions, attempted within a one-hour interval across all storage accounts in the Storage Service in a given subscription.

“Zone Redundant Storage (ZRS) Account” is a storage account for which data is replicated across multiple facilities. These facilities may be within the same geographical region or across two geographical regions.

Monthly Uptime Percentage: Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \text{Average Error Rate}$$

Service Credit – LRS, ZRS, GRS and RA-GRS (write requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Credit – RA-GRS (read requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

Service Credit – LRS, GRS and RA-GRS (write requests) Blob Storage Accounts (Cool Access Tier):

Monthly Uptime Percentage	Service Credit
< 99%	10%
< 98%	25%

Service Credit – RA-GRS (read requests) Blob Storage Accounts (Cool Access Tier):

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 98%	25%

[Table of Contents / Definitions](#)

Stream Analytics – API Calls

Additional Definitions:

“Total Transaction Attempts” is the total number of authenticated REST API requests to manage a streaming job within the Stream Analytics Service by Customer during a billing month for a given Microsoft Azure subscription.

“Failed Transactions” is the set of all requests within Total Transaction Attempts that return an Error Code or otherwise do not return a Success Code within five minutes from Microsoft’s receipt of the request.

“Monthly Uptime Percentage” for API calls within the Stream Analytics Service is represented by the following formula:

$$\text{Monthly Uptime \%} = \frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Stream Analytics – Jobs

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given job has been deployed within the Stream Analytics Service during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all jobs deployed by Customer in a given Microsoft Azure subscription during a billing month.

Downtime is the total accumulated Deployment Minutes, across all jobs deployed by Customer in a given Microsoft Azure subscription, during which the job is unavailable. A minute is considered unavailable for a deployed job if the job is neither processing data nor available to process data throughout the minute.

Monthly Uptime Percentage for jobs within the Stream Analytics Service is represented by the following formula:

[Table of Contents](#)[Introduction](#)[General Terms](#)[Service Specific Terms](#)[Appendices](#)

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Traffic Manager Service

Additional Definitions:

"Deployment Minutes" is the total number of minutes that a given Traffic Manager Profile has been deployed in Microsoft Azure during a billing month.

"Maximum Available Minutes" is the sum of all Deployment Minutes across all Traffic Manager Profiles deployed by you in a given Microsoft Azure subscription during a billing month.

"Traffic Manager Profile" or **"Profile"** refers to a deployment of the Traffic Manager Service created by you containing a domain name, endpoints, and other configuration settings, as represented in the Management Portal.

"Valid DNS Response" means a DNS response, received from at least one of the Traffic Manager Service name server clusters, to a DNS request for the domain name specified for a given Traffic Manager Profile.

Downtime: The total accumulated Deployment Minutes, across all Profiles deployed by you in a given Microsoft Azure subscription, during which the Profile is unavailable. A minute is considered unavailable for a given Profile if all continual DNS queries for the DNS name specified in the Profile that are made throughout the minute do not result in a Valid DNS Response within two seconds.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Virtual Machines

Additional Definitions:

"Announced Single Instance Maintenance" means periods of Downtime related to network, hardware, or Service maintenance or upgrades impacting Single Instances. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

"Availability Set" refers to two or more Virtual Machines deployed across different Fault Domains to avoid a single point of failure.

"Fault Domain" is a collection of servers that share common resources such as power and network connectivity.

"Single Instance" is defined as any single Microsoft Azure Virtual Machine that either is not deployed in an Availability Set or has only one instance deployed in an Availability Set.

"Virtual Machine" refers to persistent instance types that can be deployed individually or as part of an Availability Set.

"Virtual Machine Connectivity" is bi-directional network traffic between the virtual machine and other IP addresses using TCP or UDP network protocols in which the virtual machine is configured for allowed traffic. The IP addresses can be IP addresses in the same Cloud Service as the virtual machine, IP addresses within the same virtual network as the virtual machine or public, routable IP addresses.

Multiple Instance Virtual Machines

"Maximum Available Minutes" is the total accumulated minutes during a billing month for all Internet facing Virtual Machines that have two or more instances deployed in the same Availability Set. Maximum Available Minutes is measured from when at least two Virtual Machines in the same Availability Set have both been started resultant from action initiated by you to the time you have initiated an action that would result in stopping or deleting the Virtual Machines.

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Downtime: The total accumulated minutes that are part of Maximum Available Minutes that have no External Connectivity.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Single Instance Virtual Machines

"Minutes in the Month" is the total number of minutes in a given month.

Downtime: The total accumulated minutes that are part of Minutes in the Month that have no Virtual Machine Connectivity. Downtime excludes Announced Single Instance Maintenance.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated subtracting from 100% the percentage of Minutes in the Month in which any Single Instance Virtual Machine using premium storage for all disks had Downtime.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

VPN Gateway

Additional Definitions:

"Maximum Available Minutes" is the total accumulated minutes during a billing month which a given VPN Gateway has been deployed in a Microsoft Azure subscription.

"Virtual Network" refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within Microsoft Azure.

"VPN Gateway" refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

Downtime: Is the total accumulated Maximum Available Minutes during which a VPN Gateway is unavailable. A minute is considered unavailable if all attempts to connect to the VPN Gateway within a thirty-second window within the minute are unsuccessful.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Basic Gateway for VPN or ExpressRoute Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Standard Gateway for VPN or ExpressRoute / High Performance Gateway for VPN or ExpressRoute Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Visual Studio Online – Build Service

Additional Definitions:

“Build Service” is a feature that allows customers to build their applications in Visual Studio Online.

“Maximum Available Minutes” is the total number of minutes for which the paid Build Service has been enabled for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated minutes for a given Microsoft Azure subscription during which the Build Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the Build Service to perform operations initiated by you throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Visual Studio Online – Load Testing Service

Additional Definitions:

“Load Testing Service” is a feature that allows customers to generate automated tasks to test the performance and scalability of applications.

“Maximum Available Minutes” is the total number of minutes for which the paid Load Testing Service has been enabled for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated minutes for a given Microsoft Azure subscription during which the Load Testing Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the Load Testing Service to perform operations initiated by you throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Visual Studio Online – User Plans Service

Additional Definitions:

“Build Service” is a feature that allows customers to build their applications in Visual Studio Online.

“Deployment Minutes” is the total number of minutes for which a User Plan has been purchased during a billing month.

“Load Testing Service” is a feature that allows customers to generate automated tasks to test the performance and scalability of applications.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all User Plans for a given Microsoft Azure subscription during a billing month.

“User Plan” refers to the set of features and capabilities selected for a user within a Visual Studio Online account in a Customer subscription. User Plan options and the features and capabilities per User Plan are described on the <http://www.visualstudio.com> website.

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Downtime: The total accumulated Deployment Minutes, across all User Plans for a given Microsoft Azure subscription, during which the User Plan is unavailable. A minute is considered unavailable for a given User Plan if all continuous HTTP requests to perform operations, other than operations pertaining to the Build Service or the Load Testing Service, throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Microsoft Azure Services Plans

Azure Active Directory Basic

Downtime: Any period of time when users are not able to log in to the service, log in to the Access Panel, access applications on the Access Panel and reset passwords; or any period of time IT administrators are not able to create, read, write and delete entries in the directory and/or provision/de-provision users to applications in the directory.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Azure Active Directory B2C

Additional Definitions:

“Deployment Minutes” is the total number of minutes for which an Azure AD B2C directory has been deployed during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Azure AD B2C directories in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated minutes across all Azure AD B2C directories deployed by Customer in a given Microsoft Azure subscription during which the Azure AD B2C service is unavailable. A minute is considered unavailable if either all attempts to process user sign-up, sign-in, profile editing, password reset and multi-factor authentication requests, or all attempts by developers to create, read, write and delete entries in a directory, fails to return tokens or valid Error Codes, or do not return responses within two minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: No SLA is provided for the Free tier of Azure Active Directory B2C.

[Table of Contents / Definitions](#)

Azure Active Directory Premium

Downtime: Any period of time when users are not able to log in to the service, log in to the Access Panel, access applications on the Access Panel and reset passwords; or any period of time IT administrators are not able to create, read, write and delete entries in the directory and/or provision/de-provision users to applications in the directory.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Azure Information Protection Premium

Downtime: Any period of time when end users cannot create or consume IRM documents and email.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Microsoft Cloud App Security

Downtime: Any period of time when the Customer's IT administrator or users authorized by Customer are unable to log on with proper credentials. Scheduled Downtime will not exceed 10 hours per calendar year.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: This Service Level does not apply to any: (i) On-premises software licensed as part of the Service subscription, or (ii) Internet-based services (excluding Microsoft Cloud App Security) that provide updates via API (application programming interface) to any services licensed as part of the Service subscription.

[Table of Contents / Definitions](#)

Multi-Factor Authentication Service

Additional Definitions:

“Deployment Minutes” is the total number of minutes that a given Multi-Factor Authentication provider has been deployed in Microsoft Azure during a billing month.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Multi-Factor Authentication providers deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Multi-Factor Authentication providers deployed by you in a given Microsoft Azure subscription, during which the Multi-Factor Authentication Service is unable to receive or process authentication requests for the Multi-Factor Authentication provider.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Azure Site Recovery Service – On-Premises-to-Azure

Additional Definitions:

“Failover” is the process of transferring control, either simulated or actual, of a Protected Instance from a primary site to a secondary site.

“On-Premises-to-Azure Failover” is the Failover of a Protected Instance from a non-Azure primary site to an Azure secondary site. You may designate a particular Azure datacenter as a secondary site, provided that if Failover to the designated datacenter is not possible, Microsoft may replicate to a different datacenter in the same region.

“Protected Instance” refers to a virtual or physical machine configured for replication by the Azure Site Recovery Service from a primary site to a secondary site. Protected Instances are enumerated in the Protected Items tab in the Recovery Services section of the Management Portal.

“Recovery Time Objective (RTO)” means the period of time beginning when you initiate a Failover of a Protected Instance experiencing either a planned or unplanned outage for On-Premises-to-Azure replication to the time when the Protected Instance is running as a virtual machine in Microsoft Azure, excluding any time associated with manual action or the execution of your scripts.

Monthly Recovery Time Objective: The Monthly Recovery Time Objective for a specific Protected Instance configured for On-Premises-to-Azure replication in a given billing month is four hours for an unencrypted Protected Instance and six hours for an encrypted Protected Instance. One hour will be added to the monthly Recovery Time Objective for each additional 25GB over the initial 100GB Protected Instance size.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Credit (Assuming Protected Instance of 100GB, or less):

Protected Instance	Monthly Recovery Time Objective	Service Credit
Unencrypted	> 4 hours	100%
Encrypted	> 6 hours	100%

Additional Terms: Monthly Recovery Time Objective and Service Credits are calculated for each Protected Instance used by you.

[Table of Contents / Definitions](#)

Azure Site Recovery Service – On-Premises-to-On-Premises

Additional Definitions:

“Failover” is the process of transferring control, either simulated or actual, of a Protected Instance from a primary site to a secondary site.

“Failover Minutes” is the total number of minutes in a billing month during which a Failover of a Protected Instance configured for On-Premises-to-On-Premises replication has been attempted but not completed.

“Maximum Available Minutes” is the total number of minutes that a given Protected Instance has been configured for On-Premises-to-On-Premises replication by the Azure Site Recovery Service during a billing month.

“On-Premises-to-On-Premises Failover” is the Failover of a Protected Instance from a non-Azure primary site to a non-Azure secondary site.

“Protected Instance” refers to a virtual or physical machine configured for replication by the Azure Site Recovery Service from a primary site to a secondary site. Protected Instances are enumerated in the Protected Items tab in the Recovery Services section of the Management Portal.

Downtime: The total accumulated Failover Minutes in which the Failover of a Protected Instance is unsuccessful due to unavailability of the Azure Site Recovery Service, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Additional Terms: Monthly Recovery Time Objective and Service Credits are calculated for each Protected Instance used by you.

[Table of Contents / Definitions](#)

StorSimple Service

Additional Definitions:

“Backup” is the process of backing up data stored on a registered StorSimple device to one or more associated cloud storage accounts within Microsoft Azure.

“Cloud Tiering” is the process of transferring data from a registered StorSimple device to one or more associated cloud storage accounts within Microsoft Azure.

“Deployment Minutes” is the total number of minutes during which a Managed Item has been configured for Backup or Cloud Tiering to a StorSimple storage account in Microsoft Azure.

“Failure” means the inability to fully complete a properly configured Backup, Tiering, or Restoring operation due to unavailability of the StorSimple Service.

“Managed Item” refers to a volume that has been configured to Backup to the cloud storage accounts using the StorSimple Service.

“Maximum Available Minutes” is the sum of all Deployment Minutes across all Managed Items for a given Microsoft Azure subscription during a billing month.

“Restoring” is the process of copying data to a registered StorSimple device from its associated cloud storage account(s).

Downtime: The total accumulated Deployment Minutes across all Managed Items configured for Backup or Cloud Tiering by you in a given Microsoft Azure subscription during which the StorSimple Service is unavailable for the Managed Item. The StorSimple Service is considered unavailable for a given Managed Item from the first Failure of a Backup, Cloud Tiering, or Restoring operation with respect to the Managed Item

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

until the initiation of a successful Backup, Cloud Tiering, or Restoring operation of the Managed Item, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes}-\text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents](#) / [Definitions](#)

Other Online Services

Bing Maps Enterprise Platform

Downtime: Any period of time when the Service is not available as measured in Microsoft's data centers, provided that you access the Service using the methods of access, authentication and tracking methods documented in the Bing Maps Platform SDKs.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to Bing Maps Enterprise Platform purchased through Open Value and Open Value Subscription volume licensing agreements.

Service Credits will not apply if: (i) you fail to implement any Services updates within the time specified in the Bing Maps Platform API's Terms of Use; and (ii) you do not provide Microsoft with at least ninety (90) days' advance notice of any known significant usage volume increase, with significant usage volume increase defined as 50% or more of the previous month's usage.

[Table of Contents](#) / [Definitions](#)

Bing Maps Mobile Asset Management

Downtime: Any period of time when the Service is not available as measured in Microsoft's data centers, provided that you access the Service using the methods of access, authentication and tracking methods documented in the Bing Maps Platform SDKs.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to Bing Maps Enterprise Platform purchased through Open Value and Open Value Subscription volume licensing agreements.

Service Credits will not apply if: (i) you fail to implement any Services updates within the time specified in the Bing Maps Platform API's Terms of Use; and (ii) you do not provide Microsoft with at least ninety (90) days' advance notice of any known significant usage volume increase, with significant usage volume increase defined as 50% or more of the previous month's usage.

[Table of Contents / Definitions](#)

Microsoft Flow

Downtime: Any period of time when users' flows have no connectivity to Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: No SLA is provided for any free of charge tier of Microsoft Flow.

[Table of Contents / Definitions](#)

Microsoft Intune

Downtime: Any period of time when the Customer's IT administrator or users authorized by Customer are unable to log on with proper credentials. Scheduled Downtime will not exceed 10 hours per calendar year.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{User Minutes} - \text{Downtime}}{\text{User Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Service Level Exceptions: This Service Level does not apply to any: (i) On-premises software licensed as part of the Service subscription, or (ii) Internet-based services (excluding Microsoft Intune Service) that provide updates to any on-premise software licensed as part of the Service subscription.

[Table of Contents / Definitions](#)

Microsoft PowerApps

Downtime: Any period of time when users are unable to read or write any portion of data in Microsoft PowerApps to which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: No SLA is provided for any free of charge tier of Microsoft PowerApps.

[Table of Contents / Definitions](#)

Minecraft: Education Edition

Downtime: Any period of time when users are unable to access Minecraft: Education Edition.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Power BI Embedded

Deployment Minutes: is the total number of minutes for which a given workspace collection has been provisioned during a billing month.

Maximum Available Minutes: is the sum of all Deployment Minutes across all workspace collections provisioned by a customer in a given Microsoft Azure subscription during a billing month.

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Downtime: is the total accumulated Deployment Minutes, during which the workspace collection is unavailable. A minute is considered unavailable for a given workspace collection if all continuous attempts within the minute to read or write any portion of Power BI Embedded data result in an Error Code or do not return a response within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

[Table of Contents / Definitions](#)

Power BI Pro

Downtime: Any period of time when users are unable to read or write any portion of Power BI data to which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

Translator API

Downtime: Any period of time when users are not able to perform translations.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[Table of Contents / Definitions](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Service Specific Terms](#)



[Appendices](#)

Windows Desktop Operating System

Additional Definitions:

"Maximum Available Minutes" is the total accumulated minutes during a billing month for Windows Defender Advanced Threat Protection portal. Maximum Available Minutes is measured from when the Tenant has been created resultant from successful completion of the on-boarding process.

"Tenant" represents Windows Defender Advanced Threat Protection customer specific cloud environment.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes in which the Customer unable to access any portion of a Windows Defender Advanced Threat Protection portal site collections for which they have appropriate permissions and customer has a valid, active, license.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes} - \text{Downtime}}{\text{Maximum Available Minutes}} \times 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: This SLA does not apply to any trial/preview version Tenants.

[Table of Contents / Definitions](#)

[Table of Contents](#)

[Introduction](#)

[General Terms](#)

[Service Specific Terms](#)

[Appendices](#)

Appendix A – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive

With respect to Exchange Online and EOP licensed as a standalone Service or via ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for: (1) Virus Detection and Blocking, (2) Spam Effectiveness, or (3) False Positive. If any one of these individual Service Levels is not met, you may submit a claim for a Service Credit. If one Incident causes us to fail more than one SLA metric for Exchange Online or EOP, you may only make one Service Credit claim for that incident per Service.

1. Virus Detection and Blocking Service Level

- a. "Virus Detection and Blocking" is defined as the detection and blocking of Viruses by the filters to prevent infection. "Viruses" is broadly defined as known malware, which includes viruses, worms, and Trojan horses.
- b. A Virus is considered known when widely used commercial virus scanning engines can detect the virus and the detection capability is available throughout the EOP network.
- c. Must result from a non-purposeful infection.
- d. The Virus must have been scanned by the EOP virus filter.
- e. If EOP delivers an email that is infected with a known virus to you, EOP will notify you and work with you to identify and remove it. If this results in the prevention of an infection, you won't be eligible for a Service Credit under the Virus Detection and Blocking Service Level.
- f. The Virus Detection and Blocking Service Level shall not apply to:
 - i. Forms of email abuse not classified as malware, such as spam, phishing and other scams, adware, and forms of spyware, which due to its targeted nature or limited use is not known to the anti-virus community and thus not tracked by anti-virus products as a virus.
 - ii. Corrupt, defective, truncated, or inactive viruses contained in NDRs, notifications, or bounced emails.
- g. The Service Credit available for the Virus Detection and Blocking Service is: 25% Service Credit of Applicable Monthly Service Fee if an infection occurs in a calendar month, with a maximum of one claim allowed per calendar month.

2. Spam Effectiveness Service Level

- a. "Spam Effectiveness" is defined as the percentage of inbound spam detected by the filtering system, measured on a daily basis.
- b. Spam effectiveness estimates exclude false negatives to invalid mailboxes.
- c. The spam message must be processed by our service and not be corrupt, malformed, or truncated.
- d. The Spam Effectiveness Service Level does not apply to email containing a majority of non-English content.
- e. You acknowledge that classification of spam is subjective and accept that we will make a good faith estimation of the spam capture rate based on evidence timely supplied by you.
- f. The Service Credit available for the Spam Effectiveness Service is:

% of Calendar Month that Spam Effectiveness is below 99%	Service Credit
>25%	25%
> 50%	50%
100%	100%

3. False Positive Service Level

- a. "False Positive" is defined as the ratio of legitimate business email incorrectly identified as spam by the filtering system to all email processed by the service in a calendar month.
- b. Complete, original messages, including all headers, must be reported to the abuse team.
- c. Applies to email sent to valid mailboxes only.
- d. You acknowledge that classification of false positives is subjective and understand that we will make a good faith estimation of the false positive ratio based on evidence timely supplied by you.
- e. This False Positive Service Level shall not apply to:
 - i. bulk, personal, or pornographic email
 - ii. email containing a majority of non-English content
 - iii. email blocked by a policy rule, reputation filtering, or SMTP connection filtering
 - iv. email delivered to the junk folder
- f. The Service Credit available for the False Positive Service is:

False Positive Ratio in a Calendar Month	Service Credit
> 1:250,000	25%
> 1:10,000	50%

False Positive Ratio in a Calendar Month	Service Credit
> 1:100	100%

Appendix B - Service Level Commitment for Uptime and Email Delivery

With respect to EOP licensed as a standalone Service, ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for (1) Uptime and (2) Email Delivery.

1. **Monthly Uptime Percentage:**

If the Monthly Uptime Percentage for EOP falls below 99.999% for any given month, you may be eligible for the following Service Credit:

Monthly Uptime Percentage	Service Credit
<99.999%	25%
<99.0%	50%
<98.0%	100%

2. **Email Delivery Service Level:**

- a. "Email Delivery Time" is defined as the average of email delivery times, measured in minutes over a calendar month, where email delivery is defined as the elapsed time from when a business email enters the EOP network to when the first delivery attempt is made.
- b. Email Delivery Time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month.
- c. We use simulated or test emails to measure delivery time.
- d. The Email Delivery Service Level applies only to legitimate business email (non-bulk email) delivered to valid email accounts.
- e. This Email Delivery Service Level does not apply to:
 1. Delivery of email to quarantine or archive
 2. Email in deferral queues
 3. Denial of service attacks (DoS)
 4. Email loops
- f. The Service Credit available for the Email Delivery Service is:

Average Email Delivery Time (as defined above)	Service Credit
> 1	25%
> 4	50%
> 10	100%



Exhibit 4. Applicable Terms and Conditions for IBM Bluemix (formerly IBM/SoftLayer).

Service Description

IBM Bluemix

This Service Description describes IBM Bluemix Cloud Services available to Client. Client means the contracting party and its authorized users and recipients of the Cloud Service.

1. Cloud Services

IBM Bluemix includes both Platform Services and Infrastructure Services that allow Client to deploy selected services and Client content, including Client applications and data, within IBM's public Bluemix offering environment. Bluemix also supports Client's hybrid cloud strategy with Bluemix dedicated and local offerings, which allow Client to deploy selected services in a dedicated IBM data center environment or directly on Client's own local infrastructure.

Platform Services enable Client to more quickly compose, build, and deploy enterprise-grade applications by providing access to a vast portfolio of composable Cloud Services.

Infrastructure Services provide access to computing, storage, and network resources to enable Client to quickly provision or set-up cloud computing infrastructure environments.

Platform and Infrastructure Services are self-managed by Client, including selection of available data centers and selection, configuration, and management of services (such as security, backup, failover, restore, and monitoring), which Client determines are necessary to meet Client's requirements and applicable laws, including regulatory requirements for content.

1.1 Bluemix UI

Upon acceptance of Client's order and, if applicable, set-up of the dedicated or local environment, Client can use the Bluemix UI, which consists of on-line portals, mobile apps, APIs, command line interfaces, or, where available, assisted ordering (Client order placement via IBM sales support staff).

The Bluemix UI, support, and other information may be presented only in English, and the English version governs any conflict with a translation. Client is responsible for actions of Client's authorized users, including their use and associated charges for such use. Client is responsible for saving, maintaining, and protecting all access keys generated for each Cloud Service.

1.2 Cloud Service Use

Specific services and offerings within Bluemix have additional terms, such as service levels, unique security provisions, or identification of enabling software, provided in an additional Service Description or Attachment available in the Bluemix UI, which override inconsistent provisions in this Service Description. Non-IBM services are provided by the third party service provider under the provider's agreement terms as disclosed in the Bluemix UI or via a link to the provider's website. IBM is not a party to such agreements and is not responsible for the provision of or support for the third party services, even if IBM invoices for them. Client's deployment and use of the Cloud Services constitutes Client's agreement with any additional or third party terms. Client should review the additional or third party terms before placing an order or deploying the service.

IBM will provide Client at least 30 days' notice in the Bluemix UI of any changes to Service Descriptions or Attachments, or the withdrawal of a particular service. Continued use of the Cloud Services after the effective date constitutes Client's acceptance of any changed pricing or terms. IBM may enable Client to continue to use existing instances of a withdrawn service during a transition period. For those services that are identified as Tier 1 in the Bluemix UI, IBM will not withdraw the service without making a functional equivalent available or providing at least five years' notice of the withdrawal.

If IBM disables or modifies an API, IBM will use commercially reasonable efforts to provide 1) advance notice of such change and 2) continued support for prior versions of the API for a reasonable period of time, unless there are operational, legal, or security risks or burdens.

Client agrees IBM may publicly refer to Client as a subscriber to the Cloud Services in a publicity or marketing communication.

1.3 Setup and Maintenance

For Bluemix local environments, Client provides a local cloud infrastructure on Client's computers in conformance with the requirements specified in applicable Service Description or provided at

<http://www.ng.bluemix.net/docs/overview/localinfrastructure.html>, which may be updated by IBM from time to time. Client agrees to provide IBM complete access to and control over the required cloud infrastructure during the term of the Cloud Service, except as Client may need to retain access to perform mandatory maintenance and support activities on the infrastructure as described in such requirements.

IBM will maintain and update public instances of the Platform and Infrastructure Services on a regular basis during scheduled maintenance windows as published in support documentation available from the Bluemix UI portal. IBM will deploy software updates to Client's dedicated and local environments as scheduled in advance, with appropriate notification to Client, with the goal of keeping the dedicated and local environments reasonably current with the public instances as described at <http://www.ng.bluemix.net/docs/dedicated/index.html#maintainededicated.html> and <http://www.ng.bluemix.net/docs/overview/maintainlocal.html>, and in the relevant Service Description, as may be updated by IBM from time to time.

1.4 Client Solutions

Client may use the Cloud Services to create and make available to Client's end users Client solutions based on the Cloud Services. However, Client may not resell direct access to any of the Cloud Services to any third party without entering into a separate agreement with IBM. Client is responsible to have appropriate agreements in place with Client's end users, including rights to process content requested or provided by Client or Client's end users, and is responsible for their use of a Client solution. For Client's applications where Client permits Client's end users to log into Client's application using Facebook, Google, or other third party user credentials, these rights must include permission from Client's end users for IBM to receive and process all identifying information that is provided by that third party service.

Without limiting any valid indemnity claim under the "Liability and Indemnity" section of the Agreement, Client is solely responsible for any liability for damages or losses Client's end users incur as a result of using Client's solutions.

1.5 Network Access

Infrastructure Services connect to the Bluemix private network, the public network (except for services not normally exposed to the public network), and IBM's internal administrative network, and are assigned to a Client dedicated private VLAN. Client may be able to disable public network access as described in Bluemix documentation (available in the Bluemix UI). The private network enables a VPN connection for administrative access, intra-application communications, communications from different points of delivery/data centers, and for access to shared Infrastructure Service. The administrative VPN enables Client to administer and manage ordered services, and to upload, download, and manage content.

Client has no ownership or transfer rights to any IP address assigned to Client and may not use IP addresses or VLANs not assigned to Client. The IP Address Policy (available at www.softlayer.com/legal) governs use and provisioning of IP addresses, including IP addresses Client provides. If an Infrastructure Service is suspended, depending on the violation, public network or private network access may be disabled until resolution of the violation. Temporary access using the private network VLAN to remedy a violation may be available. Upon cancellation of the Cloud Services, Client must relinquish use of IP addresses, including pointing the DNS for Client's domain names away from the Cloud Services.

For Bluemix dedicated environments, Client's authorized users may access the environment through a secure VPN. IBM will provide the necessary application side, and Client will be responsible for providing the necessary user side, VPN infrastructure.

2. Security Description

2.1 Policies

Bluemix follows IBM's data security and privacy principles available at <https://www.ibm.com/cloud/resourcecenter/content/80> and any additional terms provided in this section. Any change to IBM's data security and privacy principles will not degrade the security of the Cloud Service. Client can review available Bluemix certifications at <https://www.ng.bluemix.net/docs/security/index.html> for Platform Services and <http://www.softlayer.com/compliance> for Infrastructure Services. Except for available certifications, the Cloud Service is not designed to any specific security requirements for regulated data, such as personal or sensitive personal information. Client is responsible to determine if the Cloud Services Client selects meet Client's needs with regard to the type of content Client or Client's end users may use in connection with the applicable Cloud Service or any resulting application. Client will not include any regulated content

which requires additional IBM commitments to meet regulatory requirements, such as export, privacy, or security without specific agreement from IBM.

2.2 Data Collection and Content

IBM will not access Client's or Client's end users' content except and only to extent necessary: i) when Client expressly authorizes it; ii) as specifically described in a Service Description, or a mutually agreed addendum; or iii) as required by law. In the event of a legal or governmental request for access to Client's content, and to the extent reasonably able, IBM will provide notice to Client. For content containing personal information subject to EU Data Privacy regulations, IBM's Data Processing Agreement at www.softlayer.com/legal applies.

Access to the Bluemix UI may be suspended at any time for unauthorized access or suspected misuse. Client must promptly report any security concerns, lost or stolen account information, or unauthorized access to security@softlayer.com.

3. Service Level Agreements

IBM provides service level agreements (SLAs) for IBM-branded Bluemix services. Service levels based on downtime do not include time related to exclusions, Bluemix UI unavailability, or time to reload, configure, enable, or access content or include other services indirectly affected by an outage (Downtime).

SLAs are available only if Client is compliant with the Agreement terms and do not apply to any third party including Client's end users. SLAs do not apply to beta, experimental, trial, or no-charge Cloud Services. SLAs are not a warranty and are Client's exclusive remedy for IBM's failure to meet a specified service level.

IBM will validate SLA claims based upon information provided and IBM system records. IBM will provide Bluemix UI or other notice of approved credits. IBM's reasonable determination of a credit is final. Client agrees to continue to make payment in full for Cloud Services while an SLA claim is being reviewed. Credits may not reduce payments due for a service below zero for any billing period.

If an IBM Business Partner sold Client a subscription to the Cloud Service, the monthly charge will be calculated on the then-current list price for the service that causes the SLA claim, discounted by 50%.

3.1 Exclusions

No credits will be due for failure to meet an SLA because of: scheduled or announced maintenance; problems with Client or community content, technology, designs, or instructions; non-IBM build-packs; unsupported system configurations and platforms; Client infrastructure failures, including network, hardware, facility, or power; Client system administration actions, commands, or file transfers; Client errors or failures to provide needed information or access to resolve an outage; Client-caused security incidents or Client security testing; or other causes beyond IBM's reasonable control.

For Bluemix local environments, even though the Cloud Service is designed and deployed to survive most network or hardware failures, examples of failures or events that could cause an interruption in the Cloud Service include, but are not limited to: network performance slow down; switch; data center power interruption; and disk/memory. For local environments, outages caused by these failures or events and any recovery time that would be necessary to bring the entire Cloud Service back to full operation are excluded from Downtime.

3.2 Availability SLAs

3.2.1 Platform Services

Downtime is the total accrued minutes when Client is unable to connect to any of its instances of a Platform Service and is measured from the time Client reported an outage event until the time at least one of the affected instances is available for use as validated by IBM system records. Availability, expressed as a percentage, is calculated as the total number of minutes in a contracted month minus the total number of minutes of Downtime in that month divided by the total number of minutes in that month.

IBM provides a 99.95% availability SLA for Platform Services: i) configured for high availability and distributed across multiple Bluemix public regions; or ii) provisioned across multiple dedicated or local environments in geographically separated data-centers. In addition, IBM provides a 99.5% availability service level for multiple instances of a Platform Service provisioned within a single dedicated or local environment. Client is eligible for a credit as follows:

High Availability Multiple Public Region or Multiple Dedicated/Local Environments Availability Service Level	Single Dedicated/Local Environment Availability Service Level	Credit
< 99.95%	< 99.5%	10%
< 99.90%	< 99.0%	25%

Client must submit an SLA claim by using the form at <http://ibm.biz/bluemixsupport> within seven days after the end of a contracted month providing sufficient information to identify the affected Platform Service, error messages, and other information necessary to validate the claim, referencing IBM support tickets, as applicable. The credit will be the highest applicable compensation based on the cumulative availability of the affected service during a contracted month and calculated using the monthly charges for such affected service. Credits for Platform Services cannot exceed 25% of such monthly charge.

3.2.2 Infrastructure Services

Downtime is the total accrued minutes a Client-identified Infrastructure Service is unavailable due to a service disruption based on an outage type listed below, as measured from the time of a validated outage affecting the identified service until the time such service is available, as validated by IBM support or system records.

For each 30 continuous minute period of Downtime, Client will receive a credit in the amount of 5% of the charges for the identified services directly impacted by the outage. Any period during which Downtime is less than 30 continuous minutes will not be eligible for credit. Downtime for different services may not be combined to meet this calculation.

Outage Type
Public Network
Private Network
Redundant Infrastructure Power and HVAC

Client's administrative user must submit an SLA claim ticket in the Bluemix UI portal within seven days following the end of the outage event. The ticket must identify the affected service type, IP address, dates and times of the outage period, any error messages received, contact information, and a full description of the service loss, including logs, if applicable.

3.3 Infrastructure Hardware Replacement and Upgrade SLA

IBM will use reasonable efforts to minimize Downtime when replacing failed hardware and hardware components or performing a scheduled hardware upgrade. IBM will provide the specified credit:

- for hardware replacement, except as noted below, based on the time to replace, from the time IBM verifies a Client reported hardware failure.
- for planned hardware upgrades, based on the total Downtime of the service receiving the upgrade.

Service level time periods exclude any time required to reload the operating system or applications or time service performance may be degraded.

For failure to meet a specified service level time period, Client will be eligible for a credit based on the monthly charge for the service affected by the hardware replacement or upgrade, as follows:

Service Level Time Period	Credit Percent *
≤ 2 hours	none
> 2 hours	20%
> 6 hours	40%
> 10 hours	60%
> 14 hours	80%
> 18 hours	100%

* For POWER8 servers, the service level does not apply; IBM will use commercially reasonable efforts to replace a failed server, and there is no credit for failure to meet the above service levels.

4. Technical Support

IBM provides basic level support at no additional charge for the Cloud Services. Advance support is included as part of a Bluemix dedicated or local environment for services executed within those environments. Client can select fee-based technical support offerings that provide Client additional support benefits.

Client may submit a support ticket describing the issue in accordance with the applicable support policy procedures. The support policies for Platform and Infrastructure Services are available in the Bluemix UI and provide details of available support options, as well as information on access, support business hours, severity classification, and support resources and limitations. IBM uses commercially reasonable efforts to respond to support requests; however, there is no specified response time objective for basic level support.

Unless otherwise agreed in writing, support is available only to Client (and its authorized users) and not to any end users of Client's solutions. Client is solely responsible for providing all customer support and services to its end users.

An online support forum is available at no charge at <https://developer.ibm.com/bluemix/> or on Stack Overflow at <http://stackoverflow.com/questions/tagged/bluemix>. IBM's development and support staff monitors both forums.

5. Charges

Cloud Services will be charged on a pay-as-you-go basis unless Client purchases a subscription. Service charges and pricing metrics (the units measured by the service) will be identified in the Bluemix UI or may be defined in a Service Description. The following charging models apply:

- Charges for Platform Services are generally billed in arrears and begin when the service is available for use, or for services that need to be configured by IBM based on Client input, when the service would be available for use if Client provides timely input.
- Charges for Infrastructure Services are generally billed in advance and begin upon acceptance of Client's order.
- Charges for dedicated or local environments are generally billed in advance and will be based on the specified configuration. There are no usage charges for individual services executed within a dedicated or local environment. Components may indicate a specific configured capacity (such as gigabytes or transactions per second). Since actual capacity in practice for any configuration of the Cloud Service varies depending on many factors, the actual capacity in practice may be more or less than the configured capacity.
- Usage and overage charges are based on actual usage of the specified unit of measure, and billed in arrears. Partial usage is rounded up to the next full unit of measure.
- One-time charges for a particular activity will be billed upon acceptance of an order.

5.1 Subscriptions

A Bluemix subscription provides a committed usage level over the selected subscription period for eligible services. Usage charges for services over and above the committed usage level will be billed as overage. To provide usage flexibility, subscription periods are divided into 12 month cycles (or if less than 12 months remain, the remaining number of months are a cycle). Usage credits that are paid in advance or are associated with that cycle can be used any time during that cycle for eligible services. Subscription overages will not be billed until all usage credits that are prepaid or are associated with that cycle are consumed. Usage credits unused at the end of a cycle are forfeit.

5.2 Trial Period

Client's account may be eligible for a 30-day trial period during which charges for certain eligible services are waived. Client will be charged for use of other services Client orders. If Client has administrative authority over an account, Client may upgrade from trial to production at any time. If an account is not upgraded prior to the expiration of the trial period, services in that account will be disabled until the account is upgraded.

5.3 Billing

Client will be billed charges each month by billing Client's credit card or, where available, by invoice for payment due by electronic funds transfer, or by such other method as approved by IBM.

By providing credit card information, including relevant personal data, Client agrees IBM can use such information to process payment of charges. Payment of charges will be automatic on the due date. Client is responsible to keep information current to avoid service disruption and a late payment fee of \$20 (or equivalent in local currency).

If Client believes a charge to be incorrect, Client must submit a support ticket within 30 calendar days from its due date. A credit will be provided upon validation of an incorrect charge. Client accepts billed charges for Cloud Services if not disputed within such period.

If Client requires specific funding authorization for IBM to invoice charges, such as a purchase order, Client is responsible to provide and keep such authorization timely and current with sufficient funding authorization to cover all orders submitted using Client's account credentials to avoid any service disruptions and late payment fee. Late payment fees are as specified in Client's invoice or Transaction Document.

6. Ordered Services Renewals

6.1 Subscriptions

Subscriptions automatically renew for the same term unless i) the order specifies it does not automatically renew or ii) Client provides 90 days' prior notice of its intent not to renew at the end of the subscription term.

6.2 Monthly Service Periods and Cancellation of Individual Services

Monthly service periods begin on: i) for Platform Services, the first of each calendar month; or ii) for Infrastructure Services, the IBM established account billing date, or last day of the month if that date does not exist. For monthly Infrastructure Services, to downgrade or cancel a specific service, Client must cancel using the Bluemix UI at least 24 hours prior to the end of the monthly service period (in time zone GMT-6). A service can continue to be available until the end of such monthly period and no refund or credits are provided for any unused portion. Untimely notice will result in automatic renewal for another monthly service period. Client is responsible to monitor status of any request to cancel or downgrade a service to ensure it was successful.

7. Suspension and Termination

7.1 Suspension and Termination of Individual Services

Bluemix documentation may include usage guidelines or limitations to preserve the performance, responsiveness, or integrity of the Cloud Services. Client agrees to comply with such guidelines and understands that use or applications that violate these guidelines may be suspended automatically or by IBM system administrators.

Cloud Services may be suspended if IBM reasonably determines i) a security breach exists that affects Client or the IBM infrastructure, network, or its customers or ii) Client's use may subject IBM or third party service provider to liability. Client agrees to cooperate in any investigation to resolve a suspension. Suspension will only affect the services that caused or were the basis for the suspension.

IBM will try to give reasonable advance notice of a suspension and an opportunity to remedy the cause of a suspension, unless immediate suspension is necessary to protect IBM, third party service providers, or customers of either from operational, security, or other risk, or is ordered by a court or other judicial body.

For suspended services:

- a. Client remains responsible for all charges incurred through a suspension;
- b. Client is not entitled to any SLA credits for any period of suspension; and
- c. IBM is not liable for any damages or losses Client may incur as a result of loss of access to content during a suspension.

If IBM suspends access to a service due to a material breach of Client's obligations, IBM will not reconnect the services until Client pays a \$50 reconnection fee.

IBM may terminate a Cloud Service if a suspension is not remedied within five business days from the suspension notice (or other reasonable time as may be determined by IBM).

Instances of Platform Services that are unmodified and left running in a non-billable account for 10 or more days may be suspended automatically. Any Platform Service that Client has deployed but has not used for 45 or more days in a non-billable account may be deleted.

7.2 Account Termination

Upon initial account set-up, IBM will continue to process Client's account to validate contact, account, and payment information within the initial 14 days of account activation. During this initial period, IBM may close Client's account for any reason and discontinue access to Cloud Services. IBM may terminate

Client's account for multiple violations of the Agreement terms or usage guidelines. IBM may close Client's account if no Cloud Services are ordered or remain active during any six month period.

8. General

8.1 Enabling Software

Enabling software may be provided by IBM to facilitate the use of the Cloud Service. Unless other terms are provided in a Service Description, Client may use the enabling software only in connection with use of the Cloud Service. If the enabling software contains sample code, Client has the additional right to make derivative works of the sample code and use them consistent with the above grant. The enabling software is provided subject to the applicable availability SLA, if any, but is otherwise provided AS IS.

8.2 Apple Licensed Applications

The following terms of use apply to any enabling software that runs, or is acquired from the Apple App store to run on, the Apple operating system (iOS). These terms are between Client and IBM and not with Apple. Apple is not responsible for the enabling software or the content thereof and has no obligation to furnish any maintenance or support services with respect to the enabling software.

These terms include the restrictions set forth in the App Store terms of service (<http://www.apple.com/legal/itunes/appstore/dev/stdeula/>) (Usage Rules).

If the enabling software fails to conform to any applicable warranty, Client may notify Apple, and Apple may refund any purchase price for the enabling software to Client; and, to the maximum extent permitted by applicable law, Apple will have no other warranty obligation whatsoever with respect to the enabling software.

Apple is not responsible for addressing any claims Client or a third party may have relating to, or Client's possession and/or use of, the enabling software, including, but not limited to: (i) product liability claims; (ii) any claim that the enabling software fails to conform to any applicable legal or regulatory requirement; and (iii) claims arising under consumer protection or similar legislation.

Apple is not responsible for any third party claim that the enabling software or Client's possession and use of the enabling software infringes that third party's intellectual property rights.

Any questions, complaints or claims with respect to the Apple iOS enabling software may be emailed to sales@softlayer.com.

8.3 Beta Services

Cloud Services provided as a beta or experimental service will be identified as such in the Bluemix UI and subject to the following, unless different terms are provided:

- A beta / experimental Cloud Service is provided without warranties of any kind and is provided so that Client may evaluate its functionality.
- A beta service may not be at a level of performance or compatibility of generally available services, is not fully tested, and may not comply with the normal Cloud Service security practices. Such services are not designed for use in a production environment and any such use is at Client's own risk. IBM does not guarantee it will make the beta service or any similar services generally available. If a generally available service is offered, IBM is under no obligation to offer migration capabilities or services.
- Client is responsible to pay any tax, levy, or any other charge associated with Client's use of the beta or experimental service.
- Client may use a beta service for the specified period or until IBM withdraws or terminates it. Client may terminate use of a beta service at any time. Client is responsible to remove content Client wishes to retain prior to expiration or termination of the beta service.
- IBM may suspend, limit use, change, or withdraw a beta service or change these terms without notice and at any time.
- If there are no charges, IBM's entire liability for all claims in the aggregate arising from Client's use of a beta service will not exceed the amount of any actual direct damages up to U.S. \$1,000.00 (or equivalent in local currency).
- If Client provides feedback to IBM or a third party service provider, Client agrees IBM or the third party owns and may use all feedback and suggestions provided.

Cloud Service Agreement

Using this agreement (CSA), Client may order Cloud Services from SoftLayer. As used in this CSA, "SoftLayer" means either: 1) SoftLayer Technologies, Inc., a Delaware corporation, with its principal address located at Stanford Corporate Centre, 14001 North Dallas Parkway, Suite M100, Dallas, TX 75240, for Clients registering with a principal business address in the U.S. or U.S. territories; or 2) SoftLayer Dutch Holdings B.V., Company No. 52461041, VAT No. NL 8504.55.820.B01, a Netherlands company, with its principal address at Paul van Vlissingenstraat 16, 1096BK Amsterdam, The Netherlands, for Clients registering principal business address outside the U.S. or U.S. territories. This CSA and applicable Attachments and Transaction Documents (TDs) are the complete agreement (Agreement) regarding transactions under the Agreement. If translations of the Agreement are available and there is a conflict, the English version will govern translation.

Cloud Services

A Cloud Service is an IBM branded offering hosted or managed by SoftLayer or International Business Machines Corporation (IBM) and made available via a network. Each Cloud Service is described in an Attachment or a TD, such as a Service Description (references to "IBM" in an Attachment or TD mean SoftLayer, as the selling or licensing party for the Cloud Service). Cloud Services are designed to be available 24/7, subject to maintenance. Client will be notified of scheduled maintenance. Technical support and service level commitments, if applicable, are specified in an Attachment or TD.

Client accepts an Attachment or TD by ordering, enrolling, using, or making payment for the Cloud Service. When SoftLayer accepts Client's order, SoftLayer provides Client the authorizations specified in the TD. The term, including any renewal term, for a Cloud Service is described in an Attachment or TD.

SoftLayer or IBM will provide the facilities, personnel, equipment, software, and other resources necessary to provide the Cloud Services and generally available user guides and documentation to support Client's use of the Cloud Service. Client will provide hardware, software and connectivity to access and use the Cloud Service, including any required Client-specific URL addresses and associated certificates. An Attachment or TD may have additional Client responsibilities.

Client may access a Cloud Service only to the extent of authorizations acquired by Client. Client is responsible for use of Cloud Services by any user who accesses the Cloud Service with Client's account credentials. A Cloud Service may not be used in any jurisdiction for unlawful, obscene, offensive or fraudulent content or activity, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive or deceptive messages, viruses or harmful code, or violating third party rights. If there is a complaint or notice of violation, use may be suspended until resolved, and terminated if not resolved promptly. Unless expressly provided in an Attachment or TD, Client is not authorized to use a Cloud Service to provide hosting or timesharing services to any third party.

Data Protection

Each Cloud Service is designed to protect content that Client inputs into the Cloud Service. Except for account data, Client is the sole controller for any personal data included in the content, and appoints SoftLayer as a processor to process such personal data (as those terms are defined in EU Directive 95/46/EC). Except as specified in an Attachment or TD and if SoftLayer has access to content, SoftLayer will treat content as confidential by not disclosing content other than to SoftLayer or SoftLayer affiliate employees and contractors for use only to the extent needed to deliver the Cloud Service. SoftLayer will destroy it upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request. SoftLayer may charge for certain activities performed at Client's request.

Client is responsible for obtaining all necessary permissions to use, provide, store, and process content in the Cloud Service and grants SoftLayer permission to do the same. Some of Client's content may be subject to governmental regulation or may require security measures beyond those specified by SoftLayer for an offering. Client will not input or provide such content unless SoftLayer has first agreed in writing to implement additional required security measures.

The Attachment or TD for each Cloud Service describes the security functions and features of the Cloud Service. By using the Cloud Service, Client acknowledges that it meets Client's requirements and processing instructions. SoftLayer will provide Client notice of any unauthorized third party access to Client's content of which SoftLayer becomes aware and will use reasonable efforts to remediate identified security vulnerabilities. If Client's content is lost or damaged, SoftLayer will assist Client as may be specified in the Attachment or TD, in restoring it to the Cloud Service from the last available backup copy in compatible format.

SoftLayer may use processors and subprocessors (including personnel and resources) in locations worldwide to deliver the Cloud Services. SoftLayer may transfer Client's personal data across country borders including outside the European Economic Area (EEA). A list of countries where content may be processed for an IBM Cloud Service is available at www.ibm.com/cloud/datacenters or as described in the Attachment or TD. A list of subprocessors is available upon request.

Upon request by either party, SoftLayer, Client, or their affiliates will enter into additional agreements required by law for the protection of personal data included in content, such as the standard unmodified EU Model Clauses agreement pursuant to EC Decision 2010/87/EU with optional clauses removed. The parties agree (and will procure that their respective affiliates agree), that such additional agreements will be subject to the terms of the Agreement.

SoftLayer, its affiliates, and their third party suppliers may process, store, and use account data wherever they do business to enable product features, administer use, personalize experience, and otherwise support or improve the Cloud Service account

data is all information (which may be further described in an Attachment or TD) about Client or its users provided to or collected by SoftLayer or IBM (including through tracking and other technologies, such as cookies) which is processed in accordance with the IBM Online Privacy Statement available at www.ibm.com/privacy/details/us/en/.

Changes

SoftLayer may modify a Cloud Service, without degrading its functionality or security features. Any change that affects the commercial terms (e.g. charges) of the Cloud Service will not be effective until the next agreed renewal or extension.

SoftLayer may withdraw a Cloud Service as stated in an Attachment or TD. SoftLayer will either continue to provide the Cloud Service for the remainder of Client's unexpired term, or work with Client to migrate to another Cloud Service.

Since the Agreement may apply to many future orders, SoftLayer may modify the Agreement by providing Client at least one month's written notice. Changes are not retroactive; they apply, as of the effective date, only to new orders, ongoing Cloud Services that do not expire, and renewals. For transactions with a defined renewable contract period, Client may request that SoftLayer defer the change effective date until the end of the current contract period. Client accepts changes by placing new orders or continuing use after the change effective date or allowing transactions to renew after receipt of the change notice. Except as provided above, all changes to the Agreement must be in a writing accepted by both parties. If there is a conflict, an Attachment or TD prevails over the other terms of the Agreement.

Warranties

SoftLayer warrants that it provides Cloud Services using commercially reasonable care and skill in accordance with the applicable Attachment or TD. The warranty for a Cloud Service ends when the Cloud Service ends.

SoftLayer does not warrant uninterrupted or error-free operation of a Cloud Service or that SoftLayer will correct all defects or prevent third party disruptions or unauthorized third party access. These warranties are the exclusive warranties from SoftLayer and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose. SoftLayer warranties will not apply if there has been misuse, modification, damage not caused by SoftLayer, failure to comply with instructions provided by SoftLayer, or if otherwise stated in an Attachment or TD. Non-SoftLayer or non-IBM products and services are sold under the Agreement as-is, without warranties of any kind. Third parties may provide their own warranties to Client.

Charges, Taxes, and Payment

Client agrees to pay all applicable charges specified by SoftLayer, charges for use in excess of authorizations, and any late payment fees. Prepaid Services must be used within the applicable period. SoftLayer does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid. Payment for amounts due will be as specified in an Attachment or TD.

Charges are exclusive of any customs or other duty, tax, levy, or fee imposed by any authority resulting from Client's acquisitions under the Agreement. Any such duty, tax, levy, or fee must be paid by Client. Client agrees to: i) pay withholding tax directly to the appropriate government entity where required by law; ii) notify SoftLayer prior to payment and furnish a tax certificate evidencing such payment to SoftLayer; iii) pay SoftLayer any additional amount to ensure SoftLayer receives the full amount of the charges invoiced; and iv) fully cooperate with SoftLayer in seeking a waiver or reduction of such taxes and promptly complete and file all relevant documents. If SoftLayer is legally required to pay or collect taxes for which Client is responsible, Client must pay SoftLayer the appropriate amount in addition to the amount of the charges, or provide a valid tax exemption certificate.

Liability and Indemnity

SoftLayer's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the amounts paid by Client in the previous 12 months for the service that is the subject of the claim, regardless of the basis of the claim. This limit applies collectively to SoftLayer, its affiliated entities, contractors, and suppliers. SoftLayer will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings.

The following amounts, if a party is legally liable for them, are not subject to the above cap: i) third party payments referred to in the paragraph below; ii) damages for body injury (including death); iii) damages to real property and tangible personal property; and iv) damages that cannot be limited under applicable law.

If a third party asserts a claim against Client that a Cloud Service acquired under the Agreement infringes a patent or copyright, SoftLayer will defend Client against that claim and pay amounts finally awarded by a court against Client or included in a settlement approved by SoftLayer, provided that Client promptly (i) notifies SoftLayer in writing of the claim, (ii) supplies information requested by SoftLayer, and (iii) allows SoftLayer to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts.

SoftLayer has no responsibility for claims based on non-SoftLayer products and services, items not provided by SoftLayer, or any violation of law or third party rights caused by Client's content, materials, designs, or specifications.

Termination

SoftLayer may suspend, revoke, or limit Client's use of a Cloud Service if SoftLayer determines there is a material breach of Client's obligations, a security breach, or violation of law. If the cause of the suspension can reasonably be remedied,

SoftLayer will provide notice of the actions Client must take to reinstate the Cloud Service. If Client fails to take such actions within a reasonable time, SoftLayer may terminate the Cloud Service.

Either party may terminate the Agreement: i) without cause on at least one month's notice to the other after expiration or termination of its obligations under the Agreement; or ii) immediately for cause if the other is in material breach of the Agreement, provided the one who is not complying is given notice and reasonable time to comply. Failure to pay is a material breach. Any terms that by their nature extend beyond the Agreement termination remain in effect until fulfilled, and apply to successors and assignees. Termination of the CSA does not terminate TDs, and provisions of the CSA and Attachments as they relate to such TDs remain in effect until fulfilled or otherwise terminated in accordance with their terms.

Governing Laws and Geographic Scope

Each party is responsible for complying with: i) laws and regulations applicable to its business and content; and ii) import, export, and economic sanction laws and regulations, including those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services, or data, directly or indirectly, to or for certain countries, end uses, or end users. Client is responsible for its use of SoftLayer and non-SoftLayer products and services.

Both parties agree to the application of the laws of the: i) State of New York, United States, for U.S. and U.S. territory Clients; and ii) Netherlands for all other Clients; without regard to conflict of law principles. The rights and obligations of each party are valid only in the country of Client's business address. If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect. Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under the Agreement.

General

SoftLayer is an independent contractor, not Client's agent, joint venturer, partner, or fiduciary, and does not undertake to perform any of Client's regulatory obligations, or assume any responsibility for Client's business or operations. Each party is responsible for determining the assignment of its personnel and contractors, and for their direction, control, and compensation.

SoftLayer maintains a robust set of business conduct and related guidelines covering: conflicts of interest; market abuse; anti-bribery & corruption; and fraud. SoftLayer and its personnel comply with such policies and require contractors to have similar policies.

SoftLayer resellers and IBM business partners are independent from SoftLayer and unilaterally determine their prices and terms. SoftLayer is not responsible for their actions, omissions, statements, or offerings.

Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other, except no consent is required if SoftLayer assigns to IBM or an IBM company. Assignment of SoftLayer rights to receive payments and by SoftLayer in conjunction with the sale of the portion of SoftLayer's business that includes a service is not restricted.

The Agreement applies to SoftLayer and Client and their respective Enterprise companies who avail themselves of the Agreement. The parties shall coordinate the activities of Enterprise companies under the Agreement. Enterprise companies include (i) companies within the same country that Client or SoftLayer control (by owning greater than 50% of the voting shares), (ii) any other entity that controls, is controlled by or is under common control with Client or SoftLayer and has signed a participation Attachment, and (iii) for SoftLayer IBM and its respective IBM group companies.

All notices under the Agreement must be in writing and sent as described in a TD. The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing. Any reproduction of the Agreement made by reliable means is considered an original. The Agreement supersedes any course of dealing, discussions or representations between the parties.

No right or cause of action for any third party is created by the Agreement or any transaction under it. Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose. Neither party is responsible for failure to fulfill its non-monetary obligations due to causes beyond its control. Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations. Where approval, acceptance, consent, access, cooperation or similar action by either party is required, such action will not be unreasonably delayed or withheld.

Appendix A - Country-Specific Terms

Country specific Attachments, if any, regarding data protection are available at <http://www.softlayer.com/csa>. Such data protection terms may if specified apply to Clients that select a data center within such country or geographic territory, e.g. the European Union.

In the country of Client's business address, the following terms replace or modify the referenced terms:

AMERICAS

Cloud Services

Replace the first sentence of second paragraph with:

In Latin America (all countries): Client accepts the terms in an Attachment or TD by signing it.

Charges, Taxes, Payment, and Verification

Add at the end of the second paragraph:

In Canada and United States: Where taxes are based upon the location(s) receiving the benefit of the Cloud Service, Client has an ongoing obligation to notify SoftLayer of such location(s) if different than Client's business address listed in the applicable Attachment or TD.

General

Add as a last sentence in the section:

In Canada in Province of Quebec: Both parties agree to write this document in English. Les parties ont convenu de rédiger le présent document en langue anglaise.

ASIA PACIFIC

Cloud Services

In the first sentence of the second paragraph, before the word "ordering," add:

In Hong Kong and Macau: signing (by hand or electronically),

Charges, Taxes, and Payment

In the first sentence of the second paragraph, remove the word "and" before "(iv)", and at the end of the sentence, add:

In India: – and (v) file accurate Taxes Deducted at Source (TDS) returns on a timely basis. If any tax, duty, levy or fee ("Taxes") are not charged on the basis of the exemption documentation provided by the Client and the taxation authority subsequently rules that such Taxes should have been charged, then the Client will be liable to pay such Taxes, including any interests, levies and/or penalties applicable thereon.

General

Replace the second sentence of the sixth paragraph with:

In India: Neither party will bring a legal action arising out of or related to the Agreement more than three years after the cause of action arose.

EMEA

Warranties

In the last paragraph, before the last sentence, insert the following:

In Czech Republic, Estonia, and Lithuania: , or liabilities for defects. The parties hereby exclude any liability of SoftLayer for defects beyond the agreed warranties.

Charges, Taxes, and Payment

In the first sentence, replace "specified by IBM" with the following:

In Belgium and Luxembourg: specified in or calculated in accordance with the Agreement

In the third paragraph, after the phrase: “IBM may change one-time charges without notice” add:

In Czech Republic: , though Client may terminate the Agreement if Client disagrees with the change.

Add the following to the end of the first sentence of the first paragraph:

In France: equal to the most recent European Central Bank rate plus 10 points, in addition to debt collection costs of forty (40) euros or, if these costs exceed forty euros, complementary indemnification subject to justification of the amount claimed)

In Italy: due based on SoftLayer’s notice to Client.

In Ukraine: ,on the overdue amount from the next day after the due date up to the date of actual payment, prorated for each day of delay, at the interest rate of double the discount rate determined by the National Bank of Ukraine (NBU) during the delay period (paragraph 6 of article 232 of Commercial Code of Ukraine does not apply).

Liability and Indemnity

In the first sentence of the first paragraph insert the following before the words “the amounts paid”:

In Belgium, France, Germany, Italy, Malta, Portugal, and Spain: the greater of €500,000 (five hundred thousand euro) or

In UK and Ireland: 125% of

In the first sentence of the first paragraph, replace the phrase “direct damages incurred by Client” with:

In Spain: and proven damages incurred by Client as a direct consequence of the SoftLayer default

Insert after the first sentence of the first paragraph:

In Slovakia: The total foreseeable damage shall not exceed the amount above.

Insert before the last sentence of the first paragraph:

In Russia: SoftLayer will not be liable for the forgone benefit.

In the last sentence of the first paragraph, replace “special, incidental, exemplary” with:

In France and Spain: damages to reputation

In the last sentence of the first paragraph, delete:

In Ireland and UK: economic

In the last sentence of the first paragraph, replace “indirect, or economic consequential damages” with:

In France: or indirect damages

Replace the last sentence of the first paragraph with:

In Portugal: SoftLayer will not be liable for indirect damages, including loss of profit.

In Belgium, Netherlands, and Luxembourg: IBM will not be liable for indirect or consequential damages, lost profits, business, value, revenue, goodwill, damage to reputation or anticipated savings, any third party claim against Client, and loss of (or damage to) data

In the second paragraph, delete the following:

In Hungary: and tangible personal property

In the second paragraph, replace “and (iv) damages that cannot be limited under applicable law” with the following:

In Germany: (iv) loss or damage caused by a breach of guarantee assumed by SoftLayer in connection with any transaction under the Agreement; and (v) caused intentionally or by gross negligence.

Termination

In the second paragraph, delete:

In Switzerland: Failure to pay is a material breach.

Insert the following to the end of clause “a)” before “; or”:

In Russia: without payment of any damages or penalties to the other party on the basis of early termination

Insert the following at the end:

In Netherlands: The Parties waive their rights under Title 7.1 ('Koop') and clause 7:401 and 402 of the Dutch Civil Code, and their rights to invoke a full or partial dissolution ('gehele of partiele ontbinding') of the Agreement under section 6:265 of the Dutch Civil Code

General

Add to the end the last paragraph:

In Czech Republic: Pursuant to Section to Section 1801 of Act No. 89/2012 Coll. (the “Civil Code”), Section 1799 and Section 1800 of the Civil Code as amended, do not apply to transactions under the Agreement. Client accepts the risk of a change of circumstances under Section 1765 of the Civil Code.

In Hungary: By entering into the Agreement, Client confirms that Client was sufficiently informed of all the provisions of the Agreement and had the opportunity to negotiate those terms. The following provisions may significantly deviate from the provisions generally applied by Hungarian law and both parties accept those provisions by signing the Agreement: Cloud Services; Warranty; Charges, Taxes, Payment and Verification; Liability and Indemnity, Termination; Governing Laws and Geographic Scope; and General.

Delete the following sentence in the last paragraph:

In Bulgaria, Croatia, Poland, Russia, Serbia, and Slovenia: Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose.

In the last paragraph, second sentence, replace the word “two” with:

In Latvia and Ukraine: three

In Slovakia: four

In the last paragraph, add to the end of the following sentence: “Neither party is responsible for failure to fulfil its non-monetary obligations due to causes beyond its control”:

In Russia: , including but not limited to earthquakes, floods, fires, acts of God, strikes (excluding strikes of the parties' employees), acts of war, military actions, embargoes, blockades, international or governmental sanctions, and acts of authorities of the applicable jurisdiction.

In Ukraine: , including but not limited to import, export and economic sanctions requirements of the United States.

Add the following new paragraph at the end of the document, after the signatures:

In Italy: Pursuant to the art. 1341 and 1342 of Italian Civil Code, Client expressly accepts the following articles of the Agreement: Programs; Services – Cloud Services; Services – Other Services; Machines and Appliances; Machine Code and Built in Capacity; Warranty and Post Warranty Support; Charges, Taxes, Payment and Verification; Liability and Indemnity, Termination; Governing Laws and Geographic Scope, and General.

IBM Bluemix

This Service Description describes IBM Bluemix Cloud Services available to Client. Client means the contracting party and its authorized users and recipients of the Cloud Service.

1. Cloud Services

IBM Bluemix includes both Platform Services and Infrastructure Services that allow Client to deploy selected services and Client content, including Client applications and data, within IBM's public Bluemix offering environment. Bluemix also supports Client's hybrid cloud strategy with Bluemix dedicated and local offerings, which allow Client to deploy selected services in a dedicated IBM data center environment or directly on Client's own local infrastructure.

Platform Services enable Client to more quickly compose, build, and deploy enterprise-grade applications by providing access to a vast portfolio of composable Cloud Services.

Infrastructure Services provide access to computing, storage, and network resources to enable Client to quickly provision or set-up cloud computing infrastructure environments.

Platform and Infrastructure Services are self-managed by Client, including selection of available data centers and selection, configuration, and management of services (such as security, backup, failover, restore, and monitoring), which Client determines are necessary to meet Client's requirements and applicable laws, including regulatory requirements for content.

1.1 Bluemix UI

Upon acceptance of Client's order and, if applicable, set-up of the dedicated or local environment, Client can use the Bluemix UI, which consists of on-line portals, mobile apps, APIs, command line interfaces, or, where available, assisted ordering (Client order placement via IBM sales support staff).

The Bluemix UI, support, and other information may be presented only in English, and the English version governs any conflict with a translation. Client is responsible for actions of Client's authorized users, including their use and associated charges for such use. Client is responsible for saving, maintaining, and protecting all access keys generated for each Cloud Service.

1.2 Cloud Service Use

Specific services and offerings within Bluemix have additional terms, such as service levels, unique security provisions, or identification of enabling software, provided in an additional Service Description or Attachment available in the Bluemix UI, which override inconsistent provisions in this Service Description. Non-IBM services are provided by the third party service provider under the provider's agreement terms as disclosed in the Bluemix UI or via a link to the provider's website. IBM is not a party to such agreements and is not responsible for the provision of or support for the third party services, even if IBM invoices for them. Client's deployment and use of the Cloud Services constitutes Client's agreement with any additional or third party terms. Client should review the additional or third party terms before placing an order or deploying the service.

IBM will provide Client at least 30 days' notice in the Bluemix UI of any changes to Service Descriptions or Attachments, or the withdrawal of a particular service. Continued use of the Cloud Services after the effective date constitutes Client's acceptance of any changed pricing or terms. IBM may enable Client to continue to use existing instances of a withdrawn service during a transition period. For those services that are identified as Tier 1 in the Bluemix UI, IBM will not withdraw the service without making a functional equivalent available or providing at least five years' notice of the withdrawal.

If IBM disables or modifies an API, IBM will use commercially reasonable efforts to provide 1) advance notice of such change and 2) continued support for prior versions of the API for a reasonable period of time, unless there are operational, legal, or security risks or burdens.

Client agrees IBM may publicly refer to Client as a subscriber to the Cloud Services in a publicity or marketing communication.

1.3 Setup and Maintenance

For Bluemix local environments, Client provides a local cloud infrastructure on Client's computers in conformance with the requirements specified in applicable Service Description or provided at <http://www.ng.bluemix.net/docs/overview/localinfrastructure.html>, which may be updated by IBM from time to time. Client agrees to provide IBM complete access to and control over the required cloud infrastructure during the term of the Cloud Service, except as Client may need to retain access to perform mandatory maintenance and support activities on the infrastructure as described in such requirements.

IBM will maintain and update public instances of the Platform and Infrastructure Services on a regular basis during scheduled maintenance windows as published in support documentation available from the Bluemix UI portal. IBM will deploy software updates to Client's dedicated and local environments as scheduled in advance, with appropriate notification to Client, with the goal of keeping the dedicated and local environments reasonably current with the public instances as described at <http://www.ng.bluemix.net/docs/dedicated/index.html#maintaindedicated.html> and <http://www.ng.bluemix.net/docs/overview/maintainlocal.html>, and in the relevant Service Description, as may be updated by IBM from time to time.

1.4 Client Solutions

Client may use the Cloud Services to create and make available to Client's end users Client solutions based on the Cloud Services. However, Client may not resell direct access to any of the Cloud Services to any third party without entering into a separate agreement with IBM. Client is responsible to have appropriate agreements in place with Client's end users, including rights to process content requested or provided by Client or Client's end users, and is responsible for their use of a Client solution. For Client's applications where Client permits Client's end users to log into Client's application using Facebook, Google, or other third party user credentials, these rights must include permission from Client's end users for IBM to receive and process all identifying information that is provided by that third party service.

Without limiting any valid indemnity claim under the "Liability and Indemnity" section of the Agreement, Client is solely responsible for any liability for damages or losses Client's end users incur as a result of using Client's solutions.

1.5 Network Access

Infrastructure Services connect to the Bluemix private network, the public network (except for services not normally exposed to the public network), and IBM's internal administrative network, and are assigned to a Client dedicated private VLAN. Client may be able to disable public network access as described in Bluemix documentation (available in the Bluemix UI). The private network enables a VPN connection for administrative access, intra-application communications, communications from different points of delivery/data centers, and for access to shared Infrastructure Service. The administrative VPN enables Client to administer and manage ordered services, and to upload, download, and manage content.

Client has no ownership or transfer rights to any IP address assigned to Client and may not use IP addresses or VLANs not assigned to Client. The IP Address Policy (available at www.softlayer.com/legal) governs use and provisioning of IP addresses, including IP addresses Client provides. If an Infrastructure Service is suspended, depending on the violation, public network or private network access may be disabled until resolution of the violation. Temporary access using the private network VLAN to remedy a violation may be available. Upon cancellation of the Cloud Services, Client must relinquish use of IP addresses, including pointing the DNS for Client's domain names away from the Cloud Services.

For Bluemix dedicated environments, Client's authorized users may access the environment through a secure VPN. IBM will provide the necessary application side, and Client will be responsible for providing the necessary user side, VPN infrastructure.

2. Security Description

2.1 Policies

Bluemix follows IBM's data security and privacy principles available at <https://www.ibm.com/cloud/resourcecenter/content/80> and any additional terms provided in this section. Any change to IBM's data security and privacy principles will not degrade the security of the Cloud Service. Client can review available Bluemix certifications at <https://www.ng.bluemix.net/docs/security/index.html> for Platform Services and <http://www.softlayer.com/compliance> for Infrastructure Services. Except for available certifications, the Cloud Service is not designed to any specific security requirements for regulated data, such as personal or sensitive personal information. Client is responsible to determine if the Cloud Services Client selects meet Client's needs with regard to the type of content Client or Client's end users may use in connection with the applicable Cloud Service or any resulting application. Client will not include any regulated content which requires additional IBM commitments to meet regulatory requirements, such as export, privacy, or security without specific agreement from IBM.

2.2 Data Collection and Content

IBM will not access Client's or Client's end users' content except and only to extent necessary: i) when Client expressly authorizes it; ii) as specifically described in a Service Description, or a mutually agreed addendum; or iii) as required by law. In the event of a legal or governmental request for access to Client's content, and to the extent reasonably able, IBM will provide notice to Client. For content containing personal information subject to EU Data Privacy regulations, IBM's Data Processing Agreement at www.softlayer.com/legal applies.

Access to the Bluemix UI may be suspended at any time for unauthorized access or suspected misuse. Client must promptly report any security concerns, lost or stolen account information, or unauthorized access to security@softlayer.com.

3. Service Level Agreements

IBM provides service level agreements (SLAs) for IBM-branded Bluemix services. Service levels based on downtime do not include time related to exclusions, Bluemix UI unavailability, or time to reload, configure, enable, or access content or include other services indirectly affected by an outage (Downtime).

SLAs are available only if Client is compliant with the Agreement terms and do not apply to any third party including Client's end users. SLAs do not apply to beta, experimental, trial, or no-charge Cloud Services. SLAs are not a warranty and are Client's exclusive remedy for IBM's failure to meet a specified service level.

IBM will validate SLA claims based upon information provided and IBM system records. IBM will provide Bluemix UI or other notice of approved credits. IBM's reasonable determination of a credit is final. Client agrees to continue to make payment in full for Cloud Services while an SLA claim is being reviewed. Credits may not reduce payments due for a service below zero for any billing period.

If an IBM Business Partner sold Client a subscription to the Cloud Service, the monthly charge will be calculated on the then-current list price for the service that causes the SLA claim, discounted by 50%.

3.1 Exclusions

No credits will be due for failure to meet an SLA because of: scheduled or announced maintenance; problems with Client or community content, technology, designs, or instructions; non-IBM build-packs; unsupported system configurations and platforms; Client infrastructure failures, including network, hardware, facility, or power; Client system administration actions, commands, or file transfers; Client errors or failures to provide needed information or access to resolve an outage; Client-caused security incidents or Client security testing; or other causes beyond IBM's reasonable control.

For Bluemix local environments, even though the Cloud Service is designed and deployed to survive most network or hardware failures, examples of failures or events that could cause an interruption in the Cloud Service include, but are not limited to: network performance slow down; switch; data center power interruption; and disk/memory. For local environments, outages caused by these failures or events and any recovery time that would be necessary to bring the entire Cloud Service back to full operation are excluded from Downtime.

3.2 Availability SLAs

3.2.1 Platform Services

Downtime is the total accrued minutes when Client is unable to connect to any of its instances of a Platform Service and is measured from the time Client reported an outage event until the time at least one of the affected instances is available for use as validated by IBM system records. Availability, expressed as a percentage, is calculated as the total number of minutes in a contracted month minus the total number of minutes of Downtime in that month divided by the total number of minutes in that month.

IBM provides a 99.95% availability SLA for Platform Services: i) configured for high availability and distributed across multiple Bluemix public regions; or ii) provisioned across multiple dedicated or local environments in geographically separated data-centers. In addition, IBM provides a 99.5% availability service level for multiple instances of a Platform Service provisioned within a single dedicated or local environment. Client is eligible for a credit as follows:

High Availability Multiple Public Region or Multiple Dedicated/Local Environments Availability Service Level	Single Dedicated/Local Environment Availability Service Level	Credit
< 99.95%	< 99.5%	10%
< 99.90%	< 99.0%	25%

Client must submit an SLA claim by using the form at <http://ibm.biz/bluemixsupport> within seven days after the end of a contracted month providing sufficient information to identify the affected Platform Service, error messages, and other information necessary to validate the claim, referencing IBM support tickets, as applicable. The credit will be the highest applicable compensation based on the cumulative availability of the affected service during a contracted month and calculated using the monthly charges for such affected service. Credits for Platform Services cannot exceed 25% of such monthly charge.

3.2.2 Infrastructure Services

Downtime is the total accrued minutes a Client-identified Infrastructure Service is unavailable due to a service disruption based on an outage type listed below, as measured from the time of a validated outage affecting the identified service until the time such service is available, as validated by IBM support or system records.

For each 30 continuous minute period of Downtime, Client will receive a credit in the amount of 5% of the charges for the identified services directly impacted by the outage. Any period during which Downtime is less than 30 continuous minutes will not be eligible for credit. Downtime for different services may not be combined to meet this calculation.

Outage Type
Public Network
Private Network
Redundant Infrastructure Power and HVAC

Client's administrative user must submit an SLA claim ticket in the Bluemix UI portal within seven days following the end of the outage event. The ticket must identify the affected service type, IP address, dates and times of the outage period, any error messages received, contact information, and a full description of the service loss, including logs, if applicable.

3.3 Infrastructure Hardware Replacement and Upgrade SLA

IBM will use reasonable efforts to minimize Downtime when replacing failed hardware and hardware components or performing a scheduled hardware upgrade. IBM will provide the specified credit:

- for hardware replacement, except as noted below, based on the time to replace, from the time IBM verifies a Client reported hardware failure.
- for planned hardware upgrades, based on the total Downtime of the service receiving the upgrade.

Service level time periods exclude any time required to reload the operating system or applications or time service performance may be degraded.

For failure to meet a specified service level time period, Client will be eligible for a credit based on the monthly charge for the service affected by the hardware replacement or upgrade, as follows:

Service Level Time Period	Credit Percent *
≤ 2 hours	none
> 2 hours	20%
> 6 hours	40%
> 10 hours	60%
> 14 hours	80%
> 18 hours	100%

* For POWER8 servers, the service level does not apply; IBM will use commercially reasonable efforts to replace a failed server, and there is no credit for failure to meet the above service levels.

4. Technical Support

IBM provides basic level support at no additional charge for the Cloud Services. Advance support is included as part of a Bluemix dedicated or local environment for services executed within those environments. Client can select fee-based technical support offerings that provide Client additional support benefits.

Client may submit a support ticket describing the issue in accordance with the applicable support policy procedures. The support policies for Platform and Infrastructure Services are available in the Bluemix UI and provide details of available support options, as well as information on access, support business hours, severity classification, and support resources and limitations. IBM uses commercially reasonable efforts to respond to support requests; however, there is no specified response time objective for basic level support.

Unless otherwise agreed in writing, support is available only to Client (and its authorized users) and not to any end users of Client's solutions. Client is solely responsible for providing all customer support and services to its end users.

An online support forum is available at no charge at <https://developer.ibm.com/bluemix/> or on Stack Overflow at <http://stackoverflow.com/questions/tagged/bluemix>. IBM's development and support staff monitors both forums.

5. Charges

Cloud Services will be charged on a pay-as-you-go basis unless Client purchases a subscription. Service charges and pricing metrics (the units measured by the service) will be identified in the Bluemix UI or may be defined in a Service Description. The following charging models apply:

- Charges for Platform Services are generally billed in arrears and begin when the service is available for use, or for services that need to be configured by IBM based on Client input, when the service would be available for use if Client provides timely input.
- Charges for Infrastructure Services are generally billed in advance and begin upon acceptance of Client's order.
- Charges for dedicated or local environments are generally billed in advance and will be based on the specified configuration. There are no usage charges for individual services executed within a dedicated or local environment. Components may indicate a specific configured capacity (such as gigabytes or transactions per second). Since actual capacity in practice for any configuration of the Cloud Service varies depending on many factors, the actual capacity in practice may be more or less than the configured capacity.
- Usage and overage charges are based on actual usage of the specified unit of measure, and billed in arrears. Partial usage is rounded up to the next full unit of measure.
- One-time charges for a particular activity will be billed upon acceptance of an order.

5.1 Subscriptions

A Bluemix subscription provides a committed usage level over the selected subscription period for eligible services. Usage charges for services over and above the committed usage level will be billed as overage. To provide usage flexibility, subscription periods are divided into 12 month cycles (or if less than 12 months remain, the remaining number of months are a cycle). Usage credits that are paid in advance or are associated with that cycle can be used any time during that cycle for eligible services. Subscription overages will not be billed until all usage credits that are prepaid or are associated with that cycle are consumed. Usage credits unused at the end of a cycle are forfeit.

5.2 Trial Period

Client's account may be eligible for a 30-day trial period during which charges for certain eligible services are waived. Client will be charged for use of other services Client orders. If Client has administrative authority over an account, Client may upgrade from trial to production at any time. If an account is not upgraded prior to the expiration of the trial period, services in that account will be disabled until the account is upgraded.

5.3 Billing

Client will be billed charges each month by billing Client's credit card or, where available, by invoice for payment due by electronic funds transfer, or by such other method as approved by IBM.

By providing credit card information, including relevant personal data, Client agrees IBM can use such information to process payment of charges. Payment of charges will be automatic on the due date. Client is responsible to keep information current to avoid service disruption and a late payment fee of \$20 (or equivalent in local currency).

If Client believes a charge to be incorrect, Client must submit a support ticket within 30 calendar days from its due date. A credit will be provided upon validation of an incorrect charge. Client accepts billed charges for Cloud Services if not disputed within such period.

If Client requires specific funding authorization for IBM to invoice charges, such as a purchase order, Client is responsible to provide and keep such authorization timely and current with sufficient funding authorization to cover all orders submitted using Client's account credentials to avoid any service disruptions and late payment fee. Late payment fees are as specified in Client's invoice or Transaction Document.

6. Ordered Services Renewals

6.1 Subscriptions

Subscriptions automatically renew for the same term unless i) the order specifies it does not automatically renew or ii) Client provides 90 days' prior notice of its intent not to renew at the end of the subscription term.

6.2 Monthly Service Periods and Cancellation of Individual Services

Monthly service periods begin on: i) for Platform Services, the first of each calendar month; or ii) for Infrastructure Services, the IBM established account billing date, or last day of the month if that date does not exist. For monthly Infrastructure Services, to downgrade or cancel a specific service, Client must cancel using the Bluemix UI at least 24 hours prior to the end of the monthly service period (in time zone GMT-6). A service can continue to be available until the end of such monthly period and no refund or credits are provided for any unused portion. Untimely notice will result in automatic renewal for another monthly service period. Client is responsible to monitor status of any request to cancel or downgrade a service to ensure it was successful.

7. Suspension and Termination

7.1 Suspension and Termination of Individual Services

Bluemix documentation may include usage guidelines or limitations to preserve the performance, responsiveness, or integrity of the Cloud Services. Client agrees to comply with such guidelines and understands that use or applications that violate these guidelines may be suspended automatically or by IBM system administrators.

Cloud Services may be suspended if IBM reasonably determines i) a security breach exists that affects Client or the IBM infrastructure, network, or its customers or ii) Client's use may subject IBM or third party service provider to liability. Client agrees to cooperate in any investigation to resolve a suspension. Suspension will only affect the services that caused or were the basis for the suspension.

IBM will try to give reasonable advance notice of a suspension and an opportunity to remedy the cause of a suspension, unless immediate suspension is necessary to protect IBM, third party service providers, or customers of either from operational, security, or other risk, or is ordered by a court or other judicial body.

For suspended services:

- a. Client remains responsible for all charges incurred through a suspension;
- b. Client is not entitled to any SLA credits for any period of suspension; and
- c. IBM is not liable for any damages or losses Client may incur as a result of loss of access to content during a suspension.

If IBM suspends access to a service due to a material breach of Client's obligations, IBM will not reconnect the services until Client pays a \$50 reconnection fee.

IBM may terminate a Cloud Service if a suspension is not remedied within five business days from the suspension notice (or other reasonable time as may be determined by IBM).

Instances of Platform Services that are unmodified and left running in a non-billable account for 10 or more days may be suspended automatically. Any Platform Service that Client has deployed but has not used for 45 or more days in a non-billable account may be deleted.

7.2 Account Termination

Upon initial account set-up, IBM will continue to process Client's account to validate contact, account, and payment information within the initial 14 days of account activation. During this initial period, IBM may close Client's account for any reason and discontinue access to Cloud Services. IBM may terminate Client's account for multiple violations of the Agreement terms or usage guidelines. IBM may close Client's account if no Cloud Services are ordered or remain active during any six month period.

8. General

8.1 Enabling Software

Enabling software may be provided by IBM to facilitate the use of the Cloud Service. Unless other terms are provided in a Service Description, Client may use the enabling software only in connection with use of the Cloud Service. If the enabling software contains sample code, Client has the additional right to make derivative works of the sample code and use them consistent with the above grant. The enabling software is provided subject to the applicable availability SLA, if any, but is otherwise provided AS IS.

8.2 Apple Licensed Applications

The following terms of use apply to any enabling software that runs, or is acquired from the Apple App store to run on, the Apple operating system (iOS). These terms are between Client and IBM and not with Apple. Apple is not responsible for the enabling software or the content thereof and has no obligation to furnish any maintenance or support services with respect to the enabling software.

These terms include the restrictions set forth in the App Store terms of service (<http://www.apple.com/legal/itunes/appstore/dev/stdeula/>) (Usage Rules).

If the enabling software fails to conform to any applicable warranty, Client may notify Apple, and Apple may refund any purchase price for the enabling software to Client; and, to the maximum extent permitted by applicable law, Apple will have no other warranty obligation whatsoever with respect to the enabling software.

Apple is not responsible for addressing any claims Client or a third party may have relating to, or Client's possession and/or use of, the enabling software, including, but not limited to: (i) product liability claims; (ii) any claim that the enabling software fails to conform to any applicable legal or regulatory requirement; and (iii) claims arising under consumer protection or similar legislation.

Apple is not responsible for any third party claim that the enabling software or Client's possession and use of the enabling software infringes that third party's intellectual property rights.

Any questions, complaints or claims with respect to the Apple iOS enabling software may be emailed to sales@softlayer.com.

8.3 Beta Services

Cloud Services provided as a beta or experimental service will be identified as such in the Bluemix UI and subject to the following, unless different terms are provided:

- A beta / experimental Cloud Service is provided without warranties of any kind and is provided so that Client may evaluate its functionality.
- A beta service may not be at a level of performance or compatibility of generally available services, is not fully tested, and may not comply with the normal Cloud Service security practices. Such services are not designed for use in a production environment and any such use is at Client's own risk. IBM does not guarantee it will make the beta service or any similar services generally available. If a generally available service is offered, IBM is under no obligation to offer migration capabilities or services.
- Client is responsible to pay any tax, levy, or any other charge associated with Client's use of the beta or experimental service.
- Client may use a beta service for the specified period or until IBM withdraws or terminates it. Client may terminate use of a beta service at any time. Client is responsible to remove content Client wishes to retain prior to expiration or termination of the beta service.
- IBM may suspend, limit use, change, or withdraw a beta service or change these terms without notice and at any time.
- If there are no charges, IBM's entire liability for all claims in the aggregate arising from Client's use of a beta service will not exceed the amount of any actual direct damages up to U.S. \$1,000.00 (or equivalent in local currency).
- If Client provides feedback to IBM or a third party service provider, Client agrees IBM or the third party owns and may use all feedback and suggestions provided.

Service Description

IBM Bluemix Managed Hosting

These terms are in addition to the IBM Bluemix Service Description and apply to Bluemix Infrastructure Services managed hosting service Client orders. Upon return of the Client approval of the quote, an assisted order will be placed and Client will receive notice in Bluemix UI portal that the managed hosting services are enabled.

1. Cloud Service Description

Managed hosting services assist Client in its management of Client ordered Infrastructure Services computing environments with approved configurations. Supported configurations are available upon request. A technical account manager (TAM) will be assigned to Client to serve as the initial escalation point if support processes are not sufficient to assist in communications, service requests, and delivery issue resolution.

Client is responsible for selection of services and ongoing management of the enabled computing environments, security of such environments to protect workloads and all content (including Client software), data integrity, encryption, back-up and restore, and the performance of such workloads. The following managed hosting services can be provided based upon Client specific requests as agreed by IBM and documented in a Client approved services quote.

1.1 Server Management

Selected server management services assist Client by providing monitoring and management of the specified computing environment:

- a. monitoring of servers 24x7x365 using agents that can provide daily operations reporting and interaction using on-line real-time dashboards and monthly activity reports providing availability, trouble ticket, performance, and capacity information and various performance and trend metrics. Monitoring can provide as mutually agreed:
 - up to six TCP ports (HTTP, HTTPS, SMTP, POP3, etc.) per server for service availability;
 - status events on servers and network devices including network availability, process status, file system, and capacity; and
 - key performance metrics for the operating system, select applications, and databases;
- b. notification via email or tickets to Client for monitored items when established, agreed thresholds are reached;
- c. incident management to assist with issue resolution, Client server restart, and execution of Client-provided application restart scripts;
- d. problem management to resolve infrastructure only issues and assistance to resolve recurring problems that impact infrastructure, including working with Client to develop scripts to mitigate problems when thresholds are exceeded;
- e. configuration management to assist with Client initiated configuration changes, including enabling recording of hardware configuration details in the support ticketing system, and running Client provided scripts to generate information on operating system, database, or other software configuration details (these services do not provide a configuration management database for the operating system);
- f. patch management services provide deployment and loading of Client approved patches based upon Client determined scheduling for both non-production test systems and production systems once testing is completed by Client; and
- g. TAM and system administrator may from time to time provide recommendations for Client consideration and implementation to enhance performance, capacity, and utilization based upon available data and general IT experience.

1.2 Security Management

Selected security management services assist Client by providing:

- a. set up, monitoring, and restore of Vyatta gateways, VLANs, and VPN tunnels based upon Client provided settings;
- b. monitoring of VPN concentrators (not individual VPNs) and configuration of an automated alert if a Client-provided test URL cannot be accessed; and
- c. implementation of Client specified updates to firewall rules and routing tables.

Actions taken by managed hosting support personnel documented in support tickets are performed in consultation with Client's authorized user. Client retains responsibility for logging at the operating system, including access by Client approved users, to reconcile Cloud Service system logs and service tickets.

1.3 Storage Management

Selected storage management services for local attached drives assist Client by providing monitoring of disks and scheduled replacement upon failure. These services proactively perform checks of and monitor the health of local storage drives and arrays, and provide notice of problems and scheduled replacement in the Bluemix UI portal. If Client adds additional storage to the approved computing environment and wants storage management services, Client must submit a support ticket to identify such storage devices for IBM approval. Storage management services are not available if content contains protected health or other regulated data.

2. Service Level Agreement

Managed hosting support is available 24x7x365. Client may request support by opening a support ticket via <https://console.bluemix.net> or by calling Client's TAM. Response times for a support request made via ticket or telephone will be within the following response timeframes:

Support Type	Description	Response Time Service Level
Ticket Response	Acknowledge Client questions made in tickets	Within 1 hour
Restore Request	Restore system begins if destination location is available and requested data is available in the backup repository	Within 2 hours

All responses to Client support requests will be made via support ticket, telephone call, or both, depending upon the severity of a situation and consistent with any procedures established with Client for Client's account. Resolution times are dependent on the particular circumstances and are not guaranteed. The above response time commitments do not apply to support requests made via email.

For failure to meet any of the above response time service levels in any monthly service period, Client will receive a service level credit of \$250 per event, up to 100% of the monthly recurring charges for the affected hosted system.

3. Charges

The monthly charges for managed hosting services for the approved computing environment configurations, specified in the Client approved quote loaded in Client's account profile, will be billed in advance and begin upon enablement of such services.

IBM Data Processing Addendum (with EU Standard Contractual Clauses)

(Final Version November 2016)

This Addendum is part of the Agreement for the Cloud Services between Client and the respective IBM company (IBM Contracting Party). The parties to this Addendum are (1) Client on its own behalf and on behalf of controllers (including its affiliates and third parties) that Client authorizes to use the Cloud Services, and (2) the IBM Contracting Party and the IBM companies listed in Exhibit 2 as data processors that may be used by the IBM Contracting Party to process the Client Personal Data for the purpose of providing the Cloud Services (collectively, IBM Data Processors). This Addendum has two parts: (1) the data processing terms including Exhibit 2 which apply to all IBM Data Processors; and (2) the standard contractual clauses for the transfer of personal data to processors established in third countries (Commission Decision 2010/87/EC) with optional clauses removed, attached to this Addendum as Exhibit 1 (EU Standard Contractual Clauses) which apply only to the IBM Data Processors that are established outside the European Economic Area and countries considered by the European Commission to have adequate protections as listed in table 2 of Exhibit 2.

1. Processing

- 1.1 If Client includes, or authorizes others to include, personal data in the content input into the Cloud Services or personal data is generated in performance of the Cloud Services (Client Personal Data), Client represents that it is either the data controller of the Client Personal Data or that it has, prior to agreeing to the provisions of this Addendum or extending the benefit of the Cloud Services to any new data controller, been instructed by or obtained the consent of the relevant data controller(s) to agree to the undertakings in this Addendum. Client appoints IBM Data Processors as data processors to process (as those terms are defined in EU Directive 95/46/EC, as amended or replaced, from time to time) such Client Personal Data. Client and IBM Contracting Party agree (and will procure that the data controllers and IBM Data Processors agree) that any disputes or liability under this Addendum will be subject to the limitation and exclusions of liability in the Agreement.
- 1.2 The purpose of the processing of the Client Personal Data by IBM Data Processors on behalf of Client is to provide the Cloud Services, and the subject matter, duration, and purpose are further described in the Transaction Documents and Attachments to the Agreement. The categories of data subjects, types of Client Personal Data, and processing operations and nature of processing are set out below:

Categories of Data Subjects

Unless instructed otherwise by Client, data subjects may include Client's and its affiliates' employees, contractors, business partners, other individuals, and to the extent required by law legal entities whose personal data is processed by the Cloud Services.

Types of Client Personal Data

The Client Personal Data transferred concern the following types of data:

Client determines the types of data per each Cloud Service subscribed. Client's data fields can be configured as part of the implementation of the Cloud Service or as otherwise permitted in the Cloud Service. Identified representatives of Client determine what Client Personal Data is processed based on their business processes and corresponding use of the Cloud Service. The personal data processed across all Cloud Services usually concern (a subset of) the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, and to the extent applicable legal entity information.

Processing operations and nature of processing

The Client Personal Data processed by IBM Data Processors will be subject to the following basic processing activities:

- use of Client Personal Data to provide the Cloud Services and to provide assistance to technical support
- storage of Client Personal Data in data centers
- back up of Client Personal Data
- computer processing of Client Personal Data, including data transmission, data retrieval, data access

- network access to allow Client Personal Data transfer, if required
- 1.3 Except as otherwise set out in the Agreement, the IBM Data Processors will only process Client Personal Data for the purpose of providing the Cloud Services in accordance with this Agreement. Client and IBM Data Processors shall take steps to ensure that any person acting under their authority who has access to the Client Personal Data shall not process such Client Personal Data for any other purposes, unless required to do so by applicable law.
 - 1.4 IBM Data Processors will process Client Personal Data according to Client's instructions. Client's complete and final instructions for the processing of Client Personal Data are defined by the purposes set out in Sections 1.2 and 1.3 above and this Agreement as well as Client's and its authorized users' use and configuration of features in the Cloud Service. If an additional instruction is necessary to meet mandatory legal requirements and the IBM Contracting Party is not able to accommodate the requested changes, then Client may terminate the Cloud Service by providing the IBM Contracting Party with written notice. IBM will refund any prepaid charges prorated from the termination date. Instructions given by Client have to be addressed to IBM Contracting Party and may include the correction, deletion, or blocking of Client Personal Data where the Cloud Service does not already enable Client to do so itself. Without prejudice to Client's obligations as the sole controller, if IBM Contracting Party believes Client's instruction could be violating data privacy provisions, IBM Contracting Party will inform Client without undue delay. IBM Contracting Party will be entitled to suspend the performance of the relevant instruction until Client has confirmed or modified the instruction accordingly. Client will immediately declare the confirmation or modification in writing.
 - 1.5 Client shall enter into data processing agreements with other controllers in order to allow IBM Data Processors as processors and their subprocessors to process any Client Personal Data. Client shall serve as a single point of contact for the IBM Contracting Party and is solely responsible for the internal coordination, review, and submission of instructions or requests of other controllers to the IBM Contracting Party. The IBM Contracting Party shall be discharged of its obligation to inform or notify a controller when it has provided such information or notice to Client. The IBM Contracting Party is entitled to refuse any instructions provided directly by a controller that is not Client. Similarly, the IBM Contracting Party will serve as a single point of contact for Client and is solely responsible for the internal coordination, review, and submission of instructions or requests from Client to IBM Data Processors other than IBM Contracting Party as well as for obtaining, prior to having the Cloud Services launched, all necessary permissions and regulatory approvals for such processing. If for any reason this Addendum is held to be invalid with respect to any controllers other than Client, any use of the Cloud Services by such other controllers shall be deemed authorized by Client, in the name and on behalf of Client.
 - 1.6 IBM Data Processors will comply with all data protection laws and regulations in respect of the Cloud Services applicable to data processors. IBM Contracting Party is not responsible for determining the requirements of laws applicable to Client's business or that IBM Contracting Party's provision of the Cloud Services meets the requirements of such laws. Client will not use the Cloud Services in conjunction with personal data to the extent that doing so would violate applicable data protection laws. Client will be solely responsible for the lawfulness of the agreed data processing by IBM Contracting Party, in particular for the lawfulness of the transmission of Client Personal Data to IBM Data Processors. Client confirms that it has taken into consideration professional, technical, organizational, and personal competences of the IBM Data Processors and their capability to ensure security of processed Client Personal Data when the Cloud Service was selected by Client.

2. Technical and organizational measures

- 2.1 IBM Data Processors will implement and maintain, or may enable Client to implement and maintain as described in the applicable Transaction Documents or Attachment, the following practices and procedures, which may be revised periodically, regarding the systems used to host and operate the Cloud Services:

1. Security Policies

Information security policies of the IBM group of companies (IBM) are reviewed at least annually and refined as necessary to keep current with modern threats and in line with updates to broadly accepted international standards, such as ISO/IEC 27001 and 27002.

IBM follows a mandated set of employment verification requirements for all new hires, including supplemental employees. These standards also apply to wholly owned subsidiaries and joint ventures. The requirements, which may be subject to change, include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each IBM Data Processor is responsible for implementing the above requirements in its hiring process as applicable and permissible under local law.

IBM employees are required to complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security requirements, as set out in IBM's Business Conduct Guidelines.

Security incidents are handled in accordance with IBM incident management and response policies, taking into account data breach notification requirements under applicable law.

The core functions of IBM's global cybersecurity incident management practice are conducted by IBM's Computer Security Incident Response Team (CSIRT). CSIRT is managed by IBM's Chief Information Security Office and is staffed with global incident managers and forensic analysts. National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines for computer security incident handling have informed the development and remain the foundation of IBM's global incident management processes.

CSIRT coordinates with other functions within IBM to investigate suspected incidents, and if warranted, define and execute the appropriate response plan. Upon determining that a security incident has occurred that affects Client, IBM Contracting Party will notify Client, as appropriate.

2. Access, Intervention, Transfer and Separation Control

The architecture of the Cloud Services maintains logical separation of Client Personal Data. Internal rules and measures separate data processing, such as reading, inserting, copying, amending, making available, deleting, and transferring Client Personal Data, according to the contracted purposes. Access to Client's data, including any Client Personal Data, is allowed only by authorized personnel in accordance with principles of segregation of duties, strictly controlled under identity and access management policies, and monitored in accordance with IBM's internal privileged user monitoring and auditing program.

IBM's privileged access authorization is individual, role-based, and subject to regular validation. Access to Client Personal Data is restricted to the level required to deliver services and support to Client (i.e., least required privilege).

Transfer of Client Personal Data within IBM's network takes place on wired infrastructure and behind firewalls, without the use of wireless networking.

Upon expiration or cancellation of the Cloud Services, Client Personal Data is rendered unrecoverable in conformity with NIST guidelines for media sanitization, or earlier upon Client's request.

3. Service Integrity & Availability Controls

The Cloud Services undergo penetration testing and vulnerability scanning prior to production release. Additionally, penetration testing, vulnerability scanning, and ethical hacking is performed regularly by IBM and authorized independent third parties.

Modifications to operating system resources and application software are governed by IBM change management policies. Changes to network devices and firewall rules are also governed by the change management policies and are separately assessed for security risk prior to implementation.

IBM's data center services support a variety of information delivery protocols for transmission of data over public networks, such as HTTPS, SFTP, and FTPS. IBM systematically monitors production data center

resources 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators to help detect and resolve potential exposures.

The Cloud Services have business continuity and disaster recovery plans, which are developed, maintained, verified, and tested in compliance with the ISO 27002 Code of Practice for Information Security Controls. Recovery point and time objectives for the Cloud Services are established according to their architecture and intended use and provided in the applicable TD or Attachment. Backup data intended for off-site storage, if any, is encrypted prior to transport.

Security configuration and patch management activities are performed and reviewed regularly. IBM's infrastructure is subject to emergency planning concepts, such as disaster recovery and solid disk mirroring. Business continuity plans for IBM's infrastructure are documented and regularly revalidated.

4. Activity Logging, Input Control

IBM policy requires administrative access and activity in the Cloud Services' computing environments to be logged and monitored, and the logs to be archived and retained in compliance with IBM's worldwide records management plan. Changes made to production Cloud Services are recorded and managed in compliance with IBM change management policy.

5. Physical Security, Entry Control

IBM maintains physical security standards designed to restrict unauthorized physical access to data center resources. Entry points into IBM data centers are limited, controlled by access readers, and monitored by surveillance cameras. Access is allowed only by authorized personnel.

Delivery areas and loading docks where unauthorized persons may enter the premises are strictly controlled. Deliveries are scheduled in advance and require approval by authorized personnel. Personnel who are not part of the operations, facilities, or security staff are registered upon entering the premises and are escorted by authorized personnel while on the premises.

Upon termination of employment, employees are removed from the access list and required to surrender their access badges. Use of access badges is logged.

6. Order Control

Data processing is performed only according to Client's instructions. Client's complete and final instructions for the processing of Client Personal Data are defined by Client's and its authorized users' use and configuration of the features in the Cloud Service and the purpose set out in Section 1.2 above and the Agreement, which describes the terms, functionality, support, and maintenance of a Cloud Service and measures taken to ensure the confidentiality, integrity, and availability of Client Personal Data.

7. Compliance

IBM information security standards and management practices for Cloud Services are aligned to the ISO/IEC 27001 standard for information security management and comply with the ISO/IEC 27002 Code of Practice for Information Security Controls. Assessments and audits are conducted regularly by IBM to track compliance with its information security standards. Additionally, independent third party industry standard audits are performed annually in all IBM production data centers.

- 2.2. The IBM Data Processors shall implement appropriate technical and organizational security measures as required by applicable mandatory law, which measures are incorporated by reference.
- 2.3 IBM security measures are subject to technical progress and further development. Accordingly, IBM Contracting Party reserves the right to modify the IBM security measures provided that the functionality and security of the Cloud Services are not degraded. Additional measures requested by Client will be in accordance with Section 1.4 above.

- 2.4 Client (1) confirms that the above measures provide an adequate level of protection for the Client Personal Data, and (2) will ensure that only personal data strictly required for the Cloud Service is included in the Client Personal Data.

3. Access

- 3.1 To the extent permitted by law, IBM Contracting Party will inform Client without delay of data subjects' requests for rectification, deletion, blocking of data, and enforcement of privacy rights in accordance with applicable law, complaints from data subjects, and/or objections from competent regulators. Upon notification by IBM Contracting Party, Client is responsible for handling such data subjects' requests. If Client is obliged to provide information regarding Client Personal Data to third parties (including data subjects or competent regulators), IBM will support Client to a reasonable extent, provided that (1) Client has requested IBM Contracting Party in writing and (2) Client agrees to pay the cost of any support (including internal resources) provided by IBM Contracting Party or its subcontractors (including the IBM Data Processors) based on the rates set out in IBM's price list for consulting services in excess of four hours per year.
- 3.2 IBM Contracting Party and IBM Data Processors will not disclose Client content to any unauthorized third party subject to mandatory law. If a government demands access to Client Personal Data, IBM Contracting Party will notify Client prior to disclosure unless prohibited by law.
- 3.3 IBM Contracting Party and IBM Data Processors require all personnel authorized to process Client Personal Data to commit themselves to confidentiality and complete annual security and privacy training. Such an obligation of confidentiality shall continue to be valid after termination of the Agreement and/or of their activity.
- 3.4 Client and IBM Contracting Party will inform each other without delay of any suspected non-compliance with applicable data protection laws and regulations or relevant contractual terms. Client and IBM Contracting Party will support each other in order to rectify any non-compliance as soon as reasonably practicable.

4. Audit

- 4.1 IBM Data Processors have obtained the standard security certifications and personal data seals and marks listed at the following Web pages for IBM SaaS <http://www.ibm.com/cloud-computing/built-on-cloud/saas-security> and for IBM Bluemix <https://www.ibm.com/cloud-computing/bluemix/trust-security-privacy>.
- 4.2 Upon Client's written request, IBM Contracting Party will provide Client with the most recent certifications and/or summary audit report(s) concerning the security measures for the Cloud Service or IBM computing environment used to provide the Cloud Service. IBM Contracting Party will reasonably cooperate with Client by providing available additional information to help Client better understand such security measures. To the extent it is not possible to otherwise satisfy an audit obligation mandated by applicable law, only the legally mandated entity (such as a governmental regulatory agency having oversight of Client's operations) or legally mandated functions within such entity (such as the internal controls function) may conduct an onsite visit of the facilities used to provide the Cloud Service, and only in a manner that causes minimal disruption to IBM's business and in accordance with IBM's security policies to reduce any risk to IBM's other customers. Unless mandated by law, no audits are allowed within a data center for security and compliance reasons. Client agrees to pay the costs of any support provided by IBM (including internal resources) based on the rates set out in IBM Contracting Party's price list for consulting services in excess of four hours per year.
- 4.3 To the extent permitted by applicable law, Client agrees to exercise its audit right (as set out above and, if applicable, in Clause 5 (f) of the EU Standard Contractual Clauses) by instructing IBM Data Processors to execute the audit as described in this Section 4. Changes of this instruction have to be in writing.
- 4.4 The IBM Data Processor obligations stated above in Section 4.3 and, as applicable, in Clause 12 paragraph 2 of the EU Standard Contractual Clauses shall be replaced and superseded in their entirety by the IBM Data Processors obtaining a personal data protection seal or mark, or by the adherence to a certification mechanism or a code of conduct, considered by the European Data Protection Board or the European supervisory authorities as an element to demonstrate sufficient guarantees of appropriate safeguards.

5. IBM Privacy Contact

- 5.1 The IBM privacy contact for the European Economic Area and Switzerland can be contacted at eu-mc@ie.ibm.com.

6. Return or Deletion of Client Personal Data

- 6.1 Unless otherwise required by applicable law, IBM Contracting Party will destroy the Client Personal Data upon termination or expiration of a Cloud Service within a reasonable period. However, IBM will return the Client Personal Data within a reasonable period in a reasonable and common format upon receiving written instructions from the Client prior to termination or expiration, provided that the Client Personal Data is available to IBM. IBM Contracting Party shall have no obligation to return Client Personal Data to Client if the Client Personal Data is available to Client or the other data controllers.

7. IBM Data Processors and Subprocessors

- 7.1 Client agrees that IBM Contracting Party may use the other IBM Data Processors to process the Client Personal Data in accordance with the Agreement. Client agrees that IBM Data Processors are entitled to engage subprocessors. A list of the countries where Client Personal Data may be processed is available at www.ibm.com/cloud/datacenters or as described in the applicable Transaction Documents or Attachment to the Agreement. A list of subprocessors including their addresses is available upon request. When engaging subprocessors IBM Data Processors shall conclude agreements with the subprocessors to bind them to obligations which are essentially the same as those set out in this Addendum. To the extent required, Client explicitly mandates IBM Data Processors to sign these agreements directly with the subprocessors. Client will only contact the IBM Data Processors or subprocessors in coordination with IBM Contracting Party.
- 7.2 IBM Contracting Party will notify Client in advance of any changes to IBM Data Processors or subprocessors using regular communication means such as client newsletters, websites, and portals. IBM will procure that any new data processor that is an IBM company will accede to this Addendum as new IBM Data Processor. The parties to this Addendum declare in advance that they accept such additional IBM Data Processor as a party under this Addendum and accept to be bound thereto. If Client reasonably objects to the addition of a new data processor or subprocessor (e.g., such change causes Client to be non-compliant with applicable data protection laws), Client shall notify IBM Contracting Party in writing of its specific objections within 30 days of receiving such notification. If Client does not object within such period or objects but does not terminate the Cloud Service, the addition of the new subprocessor or data processor and, if applicable, the accession to this Addendum shall be considered accepted. If Client does object to the addition of a new data processor or subprocessor and IBM cannot accommodate Client's objection, Client may terminate the Cloud Service in writing within 60 days of receiving IBM's notification. For the avoidance of doubt, the IBM Contracting Party will not allow the new subprocessor or data processor to process Client Personal Data until the subprocessor or data processor is accepted by Client or the Cloud Service is terminated in accordance with this Section 7.2.

8. Transborder Data Processing

- 8.1 If IBM Data Processors are located outside of the European Economic Area or countries considered by the European Commission to have adequate protections (Data Importers), Client and Data Importers agree that by signing this Addendum they have entered into the EU Standard Contractual Clauses. Client will procure that each controller will accede to the EU Standard Contractual Clauses. In the event of a conflict between this Addendum and the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail. If required by relevant data protection authorities, IBM Contracting Party will cause Data Importers to enter into a separate, stand-alone Standard Contractual Clauses agreement with Client. If Client is a data processor in respect of the Client Personal Data, then Client will procure that the data controller(s) in respect of the Client Personal Data will enter into a separate data transfer agreement (including the EU Standard Contractual Clauses) available from eu-mc@ie.ibm.com.

9. Security Incidents

- 9.1 IBM Contracting Party will notify Client without undue delay after becoming aware of a breach of security in respect of the Cloud Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Personal Data transmitted, stored, or otherwise processed by any IBM Data Processor ("Personal Data Breach"). IBM Contracting Party will promptly investigate the Personal Data

Breach if it occurred on IBM IT infrastructure and will assist Client upon request by providing relevant information that Client requires to meet its mandatory legal obligations (including obligations to notify supervisory authorities or data subjects), if any, in relation to the Personal Data Breach, taking into account the nature of the processing and the information available to the IBM Contracting Party. IBM Contracting Party shall have no obligation to provide such information to Client in the event such information is available to Client from sources other than IBM.

10. Applicable Law and Forum, Duration

- 10.1 Without prejudice to Clause 9 and the rights of the data subjects and national supervisory authorities under the EU Standard Contractual Clauses, Client and IBM Data Processors agree that (1) governing law of this Addendum, and (2) the forum for all disputes in respect of this Addendum, shall be the same as set out in the Agreement, unless otherwise required by applicable law.
- 10.2 If the EU Standard Contractual Clauses apply, nothing in this Addendum varies or modifies the EU Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the EU Standard Contractual Clauses.
- 10.3 This Addendum shall have an indefinite duration except that the main body shall be valid until 24 May 2018 after which date it shall cease to apply.

11. Country Required Terms

- 11.1 For transactions performed in the countries specified below, the following terms replace or modify the referenced terms in this Addendum. All terms in this Addendum that are not changed by these amendments remain unchanged and in effect.

11.2 Mandatory Security Measures

In respect of controllers established in the following countries, the reference to appropriate technical and organizational security measures required by applicable law in Section 2.2 are replaced by:

- a. in **Croatia**: Croatian Personal Data Protection Act - Article 10 (3);
 - b. in **Czech Republic**: Act. No. 101/2000 Coll. on Protection of Personal Data, as further amended;
 - c. in **Denmark**: If Client is a data controller subject to the Danish Act on Processing of Personal Data, the rules of the Executive Order on Security also apply to the processing by the IBM Data Processors. Further, any IBM Data Processor established in a different EEA Member State than Denmark is subject to the provisions on security measures laid down by law in the EEA Member State in which the IBM Data Processor is established;
 - d. in **Italy**: Annex B to D.Lgs. 196/2003;
 - e. in **Latvia**: Republic of Latvia Cabinet of Ministers Regulations No.40 of 30 January 2001 "Mandatory Technical and Organizational Requirements for Protection of Personal Data Processing";
 - f. in **Lithuania**: General Requirements for Organisational and Technical Data Security Means approved by Order No. 1T-74(1.12.E) of 18 December 2013 of the Director of the Inspectorate;
 - g. in **Poland**: Act of the Polish Parliament from August 29, 1997 on the Protection of Personal Data and the regulation of April 29, 2004 by the Minister of Internal Affairs and Administration as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing;
 - h. in **Slovakia**: Act No. 122/2013 Coll. On Protection of Personal Data, as further amended;
 - i. in **Spain**: Title VIII of the Spanish Royal Decree 1720/2007, which approves the regulation implementing the Organic Law 15/1999 on the protection of personal data; and
 - j. in **Switzerland**: Ordinance to the Federal Act on Data Protection of 14 June 1993.
- 11.3 In respect of data controllers established in **Italy**, the Client appoints the IBM Contracting Party as System Administrator (and explicitly mandates the IBM Contracting Party to appoint the IBM Data Processors as System Administrators), where the Cloud Service involves activities relating to system administrators, in accordance with the requirements of the General Provision of the Data Protection Authority of 27 November

2008 "Measures and provisions laid down for Data Controllers in respect of data processed using electronic means in connection with the attribution of functions of system administrator" as modified by Provision 25 June 2009 (Provisions), and in respect of this appointment the IBM Contracting Party (and the IBM Data Processors, if any) undertakes to comply with the following requirements:

1. to identify on an individual basis the employees acting as System Administrators with reference to the contract, with an analytic listing of the operational areas permitted on the basis of the authorization profile assigned, with reference to the Cloud Service;
2. to carefully assess the subjective characteristics of the individual (such as assessing the experience, skills and reliability) to whom it is intended to grant the title of System Administrator, with reference to the Cloud Service;
3. to make available to the Data Protection Authority, where necessary, or to the controller at the request of the latter, the information required to identify those individuals acting as "*system administrators*", including a list of the functions committed to them with reference to the Cloud Service;
4. to prepare a plan for verification of the work of System Administrators (at least yearly), with reference to the Cloud Service, in order to ensure monitoring the extent to which their work complies with the measures contained in the Provisions;
5. where the systems and/or archives are under IBM Contracting Party's (or IBM Data Processors') control to adopt systems suitable for the registration of logical access (IT authentication) - for a period not shorter than 6 months - to processing systems and electronic archives by the System Administrators, with reference to the Cloud Service, which have the characteristics provided for by the Provisions in relation to completeness, immutability and possibility of verification of their integrity.

11.4 In respect of controllers established in **Cyprus** and **Greece**, respectively, Sections 2.1(6) and 2.4 are amended by adding the following phrase to the beginning of each Section: (1) "Subject to the IBM Data Processors' obligations under art. 10 of Law 138 (I) 2001 as amended from time to time and in force" for Cyprus, and (2) "Subject to the IBM Data Processors' obligations under art. 10 of Law 2472/1997 as amended from time to time and in force" for Greece.

11.5 In respect of controllers established in **Switzerland**, references to:

- a. "EU Directive 95/46/EC" are replaced by "Federal Act on Data Protection (FADP) of 19 June 1992";
- b. "EU Standard Contractual Clauses" are replaced by "Swiss Transborder Data Flow Agreement";
- c. "Commission Decision 2010/87/EC" are replaced by "art. 6, para. 2, letter a. Federal Act on Data Protection"; and
- d. "European Data Protection Board" or "European supervisory authorities" are replaced by "Federal Data Protection and Information Commissioner";
- e. "European Commission" are replaced by "Federal Data Protection and Information Commissioner";

By signing below, Client acknowledges that it is executing this Addendum, including the EU Standard Contractual Clauses and all appendices, on its own behalf as a controller and on behalf of its affiliates or third parties as controllers which it has authorized to use the Cloud Services:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

On behalf of the data processors listed in Exhibit 2 based on powers of attorney:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

EXHIBIT 1:
EU Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

.....
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer²

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses³. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

³ This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

The parties may provide further details in an offering agreement for the Cloud Services, if required.

Data exporter

The data exporter is an entity (the “Client”) that has contracted with an affiliate of the data importers (the “IBM Contracting Party”) for the Cloud Services which allows its authorized users to enter, amend, use, delete or otherwise process personal data. Client is entering into these Clauses on its own behalf as a controller and on behalf of its affiliates or third parties as controllers authorized by Client to use the Cloud Services.

Data importer

The data importers are affiliates of the IBM Contracting Party, which provide information technology services in respect to the Cloud Services.

Data subjects

The description of categories of data subjects as set out in Section 1.2 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 1 by reference.

Categories of data

The description of types of Client Personal data as set out in Section 1.2 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 1 by reference.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

As notified by Client in writing.

Processing operations

The nature (extent and type) of the processing as set out in Section 1.2 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 1 by reference.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organizational security measures set out in clause 2.1 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 2 by reference and are binding on the data importers. The data importers have implemented and will maintain these technical and organizational security measures for the purpose of protecting Client content against accidental loss, destruction, alteration, unauthorized disclosure or access, or unlawful destruction.

EXHIBIT 2:
IBM DATA PROCESSORS (INCLUDING DATA IMPORTERS)

To be provided separately