Contract #: AR3086

STATE OF UTAH COOPERATIVE CONTRACT

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

Accenture LLP
Name

Accenture LLP c/o Marcia Richard, 818 Stewart St #400
Street Address

Seattle	WA	98101
City	*State*	*Zip*

Vendor # VC226566 Commodity Code #: 920-05 Legal Status of Contractor: Limited Liability Company

Contact *Name:* Ryan Oakes *Phone Number:* 860-756-2819 *Email:* ryan.m.oakes@accenture.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Friday, June 14, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: 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) of contract sales 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.

7. 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 Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. 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. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

Contractor's signature — Date: 6/20/19

Ryan Oakes, Managing Director
Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes
Christopher Hughes (Jun 21, 2019)

Director, Division of Purchasing — Date: Jun 21, 2019

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 Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] 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 in writing and attached to this Master Agreement as an Exhibit or Attachment.

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

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

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 services agreed to under the Master Agreement.

Data means all information, whether in oral or written (including electronic) form,

[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 PaaS.

created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

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, 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.

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 Services under this Master Agreement and billing Customers directly for such 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 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 similar 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. 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, 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.

Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination 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. 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.

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.

Product means any deliverable under this Master Agreement, including Services, software, 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. 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.

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.

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 Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through 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 statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval 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.

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 of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: 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 an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to 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 Contractor 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 Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor'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 Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor 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. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the

generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor 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 Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor 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 Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor 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. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity 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. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity 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.

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 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; 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.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State 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 Lead State, 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 Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State 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 and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity 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. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity 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, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. 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.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor

and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. 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. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Limitation of Liability:
Except as otherwise set forth in the Indemnification section above, the limit of liability shall be as follows:

i. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) five million dollars ($5,000,000), whichever is greater.

ii. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

iii. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

iv. The limitations of liability in this section will not apply to claims for bodily injury or death as set forth in Section 13, and Section 31 – Data Privacy when made applicable under a specific purchase order.

15. 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.

16. 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.

17. 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. The minimum acceptable limits shall be as indicated below, with Contractor responsible for any deductible, for each of the following categories:

(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/$3 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 $10,000,000 per occurrence and $10,000,000 in the aggregate and addressing network security and privacy including categories in subsection 2 above.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement Contractor agrees to provide thirty (30) calendar days written notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity.

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, and (2) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Accenture also agrees to provide thirty (30) days written notice of any material alteration, cancellation, non-renewal , or expiration of the coverage contained in this Agreement. 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, required limits of liability, and required endorsements) 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 or expand Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

18. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

19. 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.

20. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. 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.

c. 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 supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

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

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

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(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 order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of 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 Order.

h. Orders must be placed pursuant to this Master Agreement 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.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. 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.

21. Participants and Scope

a. Contractor may not deliver 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 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 Orders, governing law and venue relating to Orders by a Participating Entity, 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 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 services accessed 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[3].

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. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the 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

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

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 goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

22. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

23. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on 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 not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual 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 Data they will be handling.

24. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

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

26. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
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 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.

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.

27. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and 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. 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, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

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 inconsistent with the terms of the Master Agreement or orders or 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 that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

28. 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 proposal.

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. 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 based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

29. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

30. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

31. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with 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 SLA or Statement of Work.

32. Warranty: At a minimum the Contractor must warrant the following:

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

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Services it acquires from this Master Agreement.

e. 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.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

33. 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. 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 no additional cost to the Purchasing Entity. 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 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 required by the Purchasing Entity.

34. Waiver of Breach: Failure of the 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 Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by 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.

35. 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 goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or 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.

36. 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 Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

37. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA 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 services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

38. 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 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 RFP, 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 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. 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.

39. 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 Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the 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.

40. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER 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 goods and 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.

41. Contract Provisions for 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, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

42. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

43. 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://calculator.naspovaluepoint.org. 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 H.

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.

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.

44. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO

ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. 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.

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

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
IaaS	Yes	Yes	Yes	Private Cloud, Public Cloud, Hybrid Cloud
PaaS	Yes	Yes	Yes	Private Cloud, Public Cloud, Hybrid Cloud
SaaS	Yes	Yes	Yes	Private Cloud, Public Cloud, Hybrid Cloud

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor: Accenture

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.
2. 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.
3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.
4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.
5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Infrastructure as a Service (IaaS)

Description	Minimum Discount % Off
IaaS Minimum Discount % * (applies to all OEM's offered within this IaaS model)	1.00%
Average IaaS OEM Discount Off	**1.00%**

Cloud Service Model: Platform as a Service (PaaS)

Description	Discount
PaaS Minimum Discount % * (applies to all OEM's offered within this PaaS model)	1.00%
Average PaaS OEM Discount Off	**1.00%**

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
OEM: Salesforce	7.00%
OEM: Accenture	10.00%
Average SaaS OEM Discount Off	**8.50%**

Additional Value Added Services

		Onsite Hourly Rate		Remote Hourly Rate	
Item Description		**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services		Defer to Accenture - Detailed Product Offering Attachment			
Professional Services					
	Deployment Services	Defer to Accenture - Detailed Product Offering Attachment			
	Integration Services)	Defer to Accenture - Detailed Product Offering Attachment			
	Consulting/Advisory Services	Defer to Accenture - Detailed Product Offering Attachment			
	Architectural Design Services	Defer to Accenture - Detailed Product Offering Attachment			
	Statement of Work Services	Defer to Accenture - Detailed Product Offering Attachment			
Partner Services		Defer to Accenture - Detailed Product Offering Attachment			
Training Deployment Services		Defer to Accenture - Detailed Product Offering Attachment			

	Deliverable Rates	
	NVP Price	**Catalog Price**
NA	NA	NA

6.0 TECHNICAL RESPONSE

Accenture's Journey to Cloud (J2C) approach applies industry know-how to help our clients swiftly and safely migrate to the cloud to unlock the business value from As-a-Service models. We provide integrated application and infrastructure services that represent a complete end-to-end offering to rapidly transform our client's IT.

With over 50,000 cloud professionals, over 20,000 cloud projects completed or underway, and over 1.6 million workloads migrated, NASPO participating entities will be in safe hands continuing their Journey to Cloud with Accenture. Accenture's comprehensive J2C approach includes three phases:

1. **Strategy, Assessment, and Roadmap**
   This phase defines the client's specific journey. Outcomes include an industry tailored cloud vision and details the value case, target state design, and delivery model according to unique preferences and needs of the client to achieve its business strategy.

2. **Cloud Transformation and Migration**
   The second phase is execution of the journey defined in the Strategy, Assessment and Roadmap phase. It delivers the cloud vision -- builds the cloud infrastructure and operating capability for business systems while migrating and/or modernizing applications to be cloud-ready, replacing with SaaS or building new cloud native applications.

3. **Cloud Management and Optimization**
   The third phase manages and operates on the cloud. It orchestrates the management of cloud applications and infrastructure operations leveraging cloud-optimized shared service delivery to deliver value and quality for clients.

The services that we describe here in our response for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) map directly to the Cloud Transformation and Migration and Cloud Management and Optimization phases of a Purchasing Entities' journey.

INFRASTRUCTURE AS A SERVICE

As part of our J2C offerings, Accenture provides a set of Infrastructure and Cloud Management and Optimization Services leveraging analytics, automation, and increasingly automatic intelligence to drive continuous operation and improvements of our customer's cloud footprint.

Our Cloud Management and Optimization services provide simultaneous management of public, private, and hybrid cloud infrastructure and applications, helping clients to manage the complexity of their hybrid IT during what can be a multi-year Journey to Cloud.

The resources we deploy to support our IaaS offerings are talented professionals well-versed in the industry, our 'Next Generation' operating model, and the various platforms that are constantly evolving. Our J2C offerings incorporate analytics, automation, and an increasing number of cognitive tools, to shift from reactive to predictive service management. Our solutions can be delivered "as a service" with utility and consumption economics, elastic capacity, industrialized delivery, and future-proofed capabilities.

In the sections that follow, we describe our IaaS abilities and approach to providing IaaS services with our Accenture Cloud Platform (ACP) and Desktop as a Service (DaaS) offerings.

Accenture Cloud Platform

The Accenture Cloud Platform (ACP) is part of Accenture Managed Services. It's a multi-cloud CMP (Cloud Managed Platform) that simplifies the complexity of the enterprise's technology landscape and enables as-a-service operations for cloud business. With ACP, organizations can create, publish, provision, manage, and govern enterprise, cross-platform (e.g., Amazon Web Services (AWS), Azure, Google, and Private Cloud) cloud resources and services, securely and effectively. Providing control and agility to manage your cloud infrastructure resources and deliver everything "as a service," at speed, and at scale. In short, ACP is a cloud environment orchestration platform.

ACP Service Offerings

- **Managed Patching** of the servers is an ongoing scheduled monthly procedure. Accenture works with you to determine the right monthly schedule for your patches. In most cases you will fit into one of the many predefined schedules; however, there are options to create specific schedules based on requirements.
- **OS Administration** is included in Managed Services. Accenture's cloud management team performs regular checks of system state and security to confirm that virtual servers and networks are protected from attacks and running optimally.
- **OS Hardening** applies ACP security standards to your virtual machines (VMs) via a set of operating system policy and configuration changes. These settings include VM policies, network settings, and security settings.
- **AV Management**: This service includes antivirus, host firewall, and intrusion detection services (IDS) and is available for supported Windows and Linux OS.
- **VM Availability Monitoring**: ACP provides the tools and infrastructure to monitor your server's resources and receive alerts.
- **Standard HP Toolset Integration for Monitoring:**
  - HP Universal Discovery for Asset Management and HP uCMDB for Configuration Management
  - HP Network Node Manager for Network availability, event, configuration, and performance management
  - Integration with AWS CloudWatch and HP SiteScope for cloud servers and other cloud alerts and application, database, and storage monitoring
  - Operations Bridge for EventCorrelation
  - Feed our IT Service Management tooling, currently based on ServiceNow
- **Cloud Provider (AWS/Azure) Native Backup and Storage Tools:** These include S3, Glacier, AMI, Snapshots, Cross Region replication, S3 level Policy-driven Backup/Archival, and Storage Gateway (Stored/Cached).
- **ACP Backup Solution:** Apart from public cloud provider native backup provisioning and support, Accenture provides and supports a cross cloud backup service enabling clients for backing up a broad range of file types, data sources, and backup modes.

- **Compliance Watch:** Compliance Watch detects and responds to security threats and alerts as they happen, combining tooling, recommended practices, and expertise for: Prevention of misconfiguration of resources (S3, public databases, public EC2 instances, security groups), Identification of potential security or CDP violations.

Supported Cloud Providers

As a vendor-neutral platform, ACP supports private and public cloud technology from a broad range of leading global providers that includes AWS, Microsoft Azure, and Google Cloud Platform. Supported private cloud platforms include Oracle Cloud and VMware vCenter. ACP's functionality and neutrality is illustrated in Figure 1.

With Accenture's deep technology skills, specialized industry knowledge, and business process expertise built into every cloud solution, our clients can achieve a new level of control, agility, and security that will help them accelerate innovation, and drive higher performance.

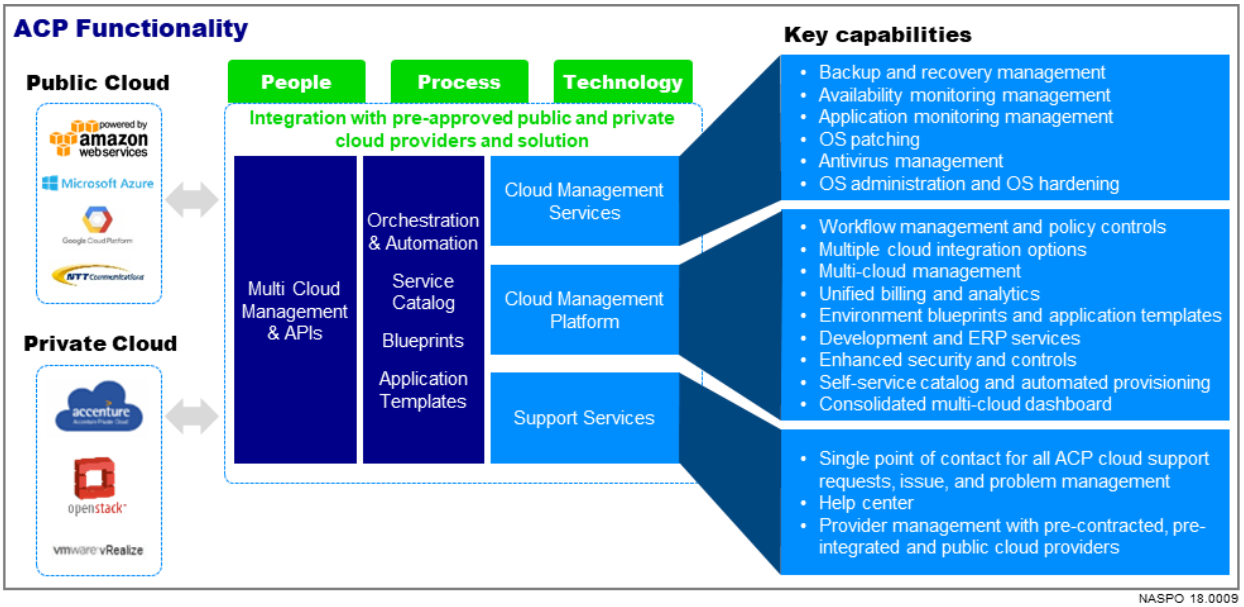


Figure 1. As a vendor-neutral platform, ACP supports private and public cloud technology from a broad range of leading global providers that includes AWS, Microsoft Azure, and Google Cloud Platform.

Compute

ACP allows automated provisioning, which allows clients to quickly and centrally create and manage cloud compute networks and virtual machines, independent of the service provider. "Compute" refers to applications and workloads that require a great deal of computation, necessitating sufficient resources to handle these computation demands in a virtual environment and in an efficient manner. Compute-intensive applications stand in contrast to data-intensive applications, which typically handle large volumes of data and as a result place a greater demand on input/output and data manipulation tasks.

Storage

Secured and efficient access to a storage volume is one of the prime requirements for any IT infrastructure. Accenture Cloud Platform resource dashboards provide multiple views to more easily access and manage cloud storage resources such as storage volumes and storage accounts.

Desktop as a Service

Accenture provides and supports desktop as-a-service (DaaS) services leveraging Amazon WorkSpaces powered by AWS. Amazon WorkSpaces provides users with a desktop experience in the cloud that can be accessed from any connected device.

PLATFORM AS A SERVICE

As part of our J2C offerings, Accenture provides a set of PaaS solutions to aid Purchasing Entities in deployment of a platform allowing them to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Accenture PaaS solutions allow Purchasing Entities to use an increasing variety of digital platforms and services to meet their business needs while providing quicker turnaround on their research, development, and go-to-market activities.

Accenture can help with the following services:

- A wide range of cloud-enabled PaaS services with managed IT services support
- Design and build PaaS services to manage the infrastructure and applications
- Application development accelerators for PaaS Platforms
- PaaS dashboard views for better visibility into resource data and operational effectiveness

Accenture is industrializing AWS PaaS services on ongoing basis. Accenture PaaS Managed Services Support includes, but is not limited to the services listed in Figure 2.

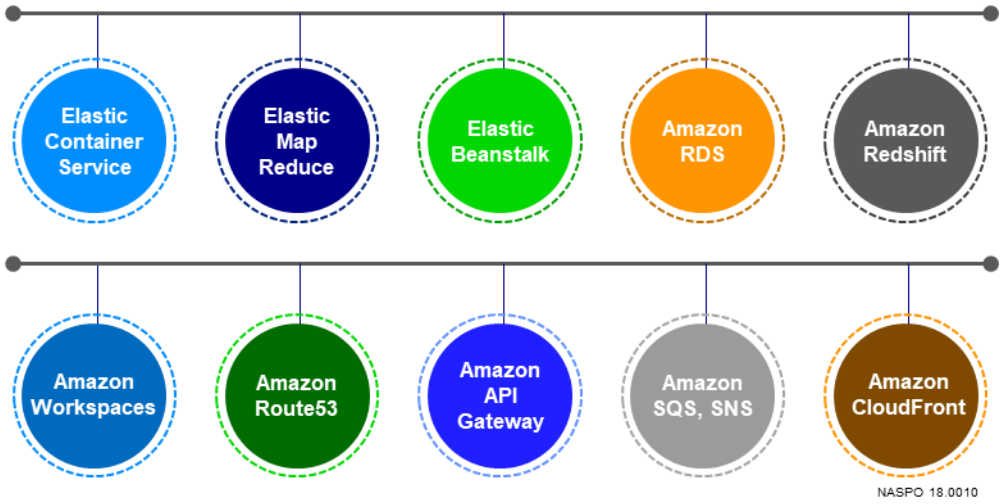


Figure 2. An example of AWS offerings that Accenture uses to provide PaaS solutions for our clients.

In the paragraphs that follow, we describe our PaaS abilities and approach to providing PaaS services with our Database as a Service (DBaaS), Accenture Reach Platform, and Salesforce Platform offerings.

Database as a Service

Database-as-a-Service (DBaaS) is the fastest growing cloud service, and the Platform-as-a-Service component provides significant improvements in productivity, performance, standardization, and data security of databases.

Accenture provides and supports the following AWS DBaaS services:

- AWS Relational Database Service (RDS)
  - Amazon Aurora
  - MYSQL
  - MSSQL
  - MariaDB
  - Oracle
  - PostgreSQL
- AWS DynamoDB
- AWS Redshift

Accenture Reach Platform

The Reach Platform provides a robust technical foundation, along with a core set of capabilities, to enable Purchasing Entities to engage their end users in a more meaningful way. This is happening within a landscape where new technologies are constantly being introduced, solutions are maturing at an accelerated pace, customer data faces growing complexities, partner ecosystems keep expanding, and new security threats that continuously arise. All of that is occurring against the backdrop of increasing customer expectations demanding services, access, functionality, and self-service options which behave, sound, and feel like commercial brands. The dynamic nature of today's world continues to put increased pressure on organizations to rapidly evolve both their user experience as well as the underlying technologies to drive it.

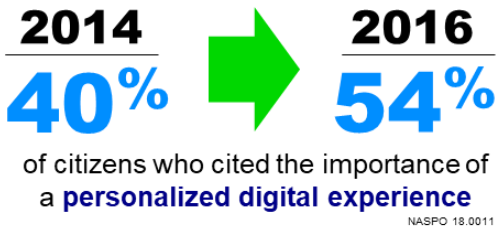


Figure 3. Accenture's Reach Platform provides a powerful digital experience, powered by a modern, cloud-native architecture, that can be used to engage an organization's end users.

In response to the myriad of challenges to effectively pivot to a "digital first" methodology and approach, Accenture continues to develop an integrated and disruptive digital government services platform upon which all end user-facing services, functionality, and capabilities can reside. According to Accenture's 2014 Public Service Pulse Survey, 40 percent of citizens cited a personalized digital experience as valuable and by 2016 that number had grown to more than half (54 percent) who pointed to the importance of personalized experiences. Customers desire intelligently personalized services and have

demonstrated the willingness to use new channels, such as chatbots and virtual assistants, that are powered by a variety of artificial intelligence technologies.

Accenture's Reach Platform, shown in Figure 4, combines a commercial-like experience, using a practical application of design thinking, with the right open source building blocks to help Purchasing Entities become more agile and deliver the digital services that users demand. While seeking to address the needs of an ever-advancing technical landscape by modernizing digital services, Purchasing Entities would benefit, not only from a modern, extensible platform, but from a partner that understands digital government and is capable of delivering technology at pace and scale.

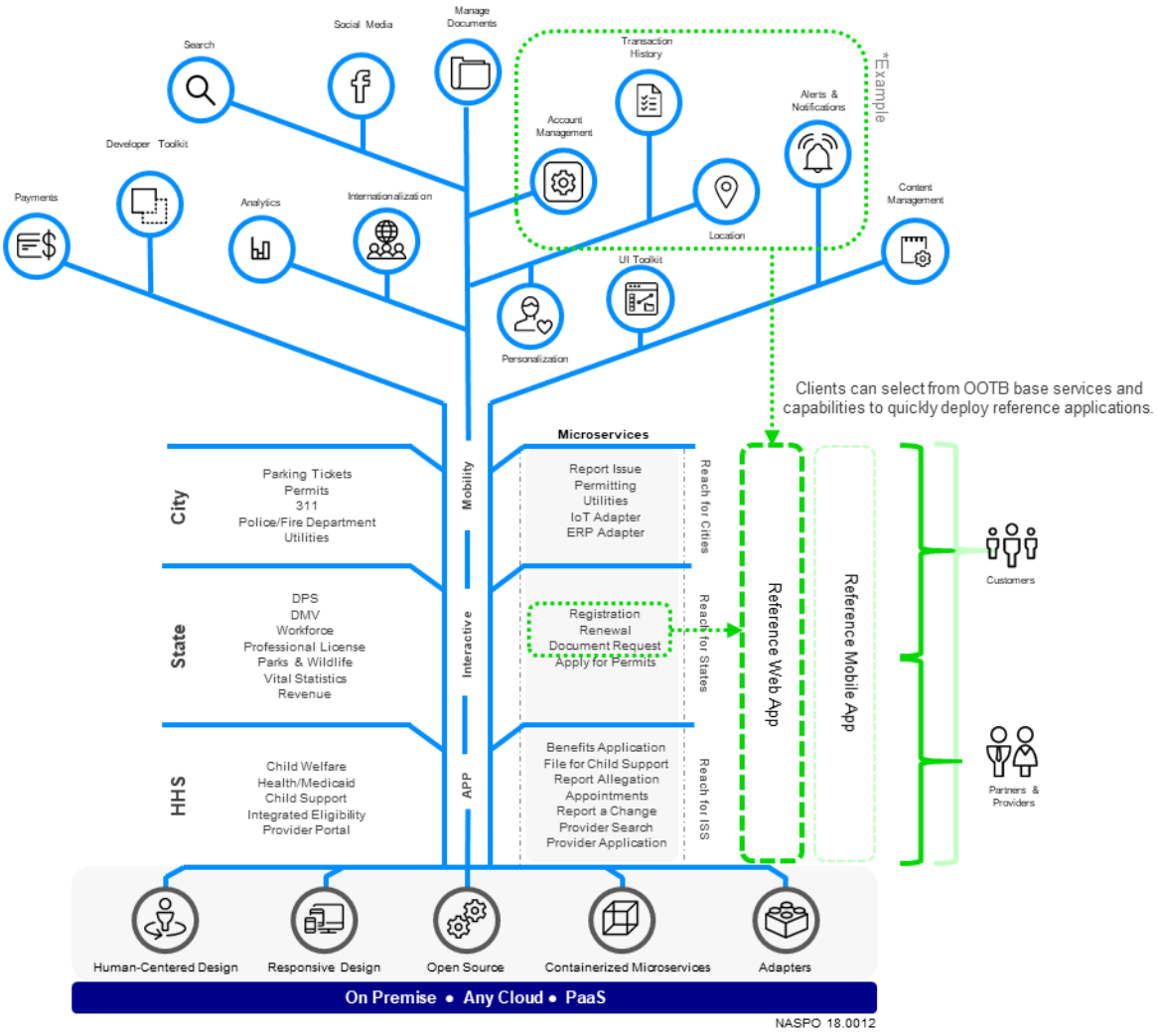


Figure 4. Accenture's Reach Platform enables modernized, scalable, and innovative digital service delivery.

The Reach community model allows the platform to continuously evolve in the same way as the customers it serves; by collaborating, sharing ongoing public investments through new capabilities, and remaining focused on delivering value to the public. We understand budgets are fixed and changing legacy backend systems is not always feasible. The Reach Platform accelerates development and speed-

to-market through reusable and extensible components that modernize end-user interactions quickly and efficiently, without impacting existing systems and technical infrastructure. Most importantly, Reach is for agency development. Open APIs allow agencies to develop their own business services specific to their constituents, similar to Facebook, Twitter and Yelp. Design, UI, and development tool kits democratizes development to help agencies self-build, while establishing standards and controls to ensure quality application development.

Salesforce Platform

Force.com is the world's largest and most extensive B2B application ecosystem in the world. Accenture is offering resale of Salesforce Platform, combined with Heroku and our implementation services, as part of a comprehensive Salesforce solution based on a customer's specific requirements and statement of work.

Accenture was one of the first to establish a strategic alliance partnership with Salesforce, and continues to strengthen its position as a leading ecosystem partner. With thousands of Salesforce implementations at more than 1,100 global enterprises, Accenture is driving Salesforce's largest transformational projects. Together, Accenture and Salesforce help clients drive innovation at scale, not only transforming all facets of their business, but industries as well.

SOFTWARE AS A SERVICE

SaaS solutions are also key components of Accenture's J2C offerings and Accenture is recognized as a leader in SaaS implementation services. Accenture SaaS offerings support Purchasing Entities with the following applications:

- Implementation of Big Data and Analytics technologies with the Accenture Insights Platform
- Deployment of a cloud-based development platform with the Accenture DevOps Platform
  - Augmentation of worker capacity and service delivery transformation using cognitive services and intelligent automation with the Accenture Virtual Assistant Platform
  - Customer Relationship Management through the industry leading Salesforce Service Cloud

Accenture uses cross-industry knowledge and experience to design, build, and grow our collection of SaaS solutions and support services in cloud-hosted, vendor-managed environments. We work with Purchasing Entities to ensure that services meet their capability needs and identify the best method to measure the effectiveness and adoption of the services.

Accenture Insights Platform

Accenture Insights Platform (AIP) is an integrated suite of leading big data and analytics technologies that comes pre-configured and 'wired together' for ease of use, speed to insight, and recommended practice security. The AIP architecture, illustrated in Figure 5, contains industry leading technologies across the

AIP solution components (layers), namely Data Ingestion, Storage, Analytics, Visualization, and Cloud (hosting). We are continuing to expand this platform to encompass new tools and capabilities.

AIP also has the Applications Design layer, which is a secure, integrated Design Studio environment to enable us to configure and build advanced analytics applications very quickly for clients, which integrates into their workflows. These applications can be run on their own or through the AIP.

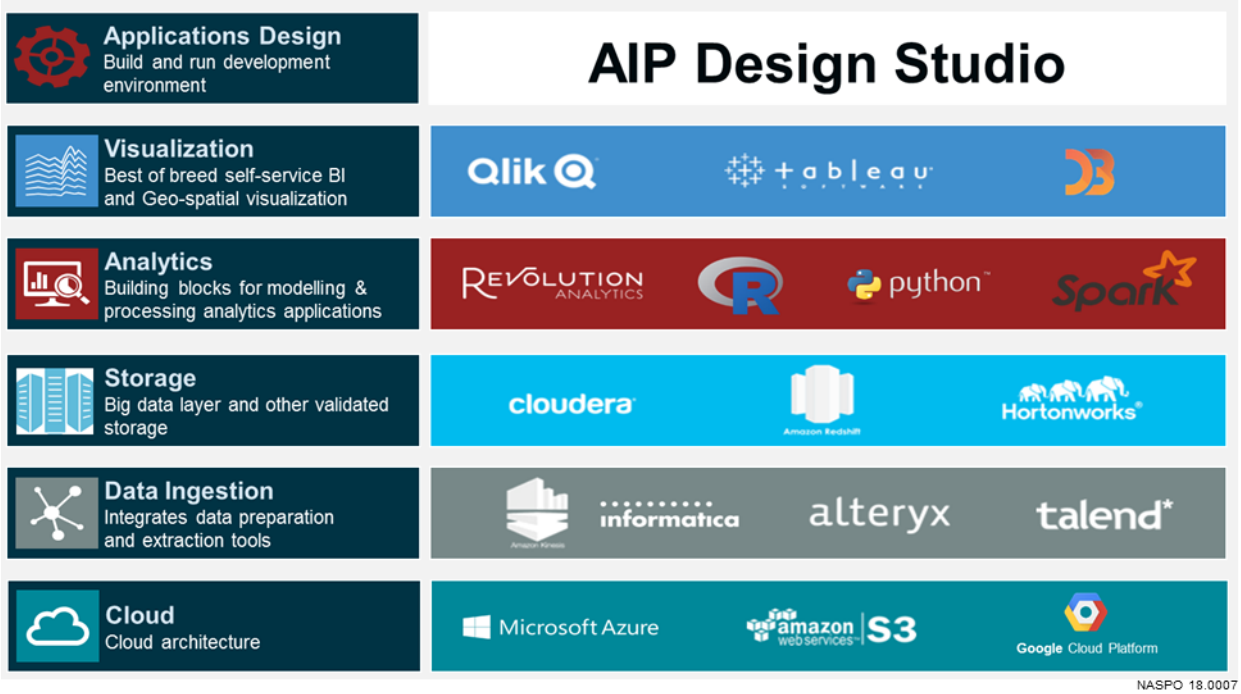


Figure 5. Accenture Insights Platform (AIP) is an integrated suite of leading big data and analytics technologies that comes pre-configured and 'wired together' for ease of use, speed to insight, and recommended practice security.

AIP is a service-enabled component based analytics solution that delivers sophisticated analytics tools, built on industry-leading technologies with an end-to end hybrid data architecture that can store varied data. 'Analytics' is not something that can be achieved with a single product. It requires many different products and software capabilities. This robust new platform can normalize data, combine the known with the unknown, and then deliver outcomes and value in ways that until now were never possible.

It is difficult for any organization with limited resources, to acquire and then build and maintain all those capabilities. With AIP, Accenture has already been licensed and offers to our clients a comprehensive and integrated suite of leading technologies, available on pay-as-you-need commercial arrangements and user support. Our goal is to help our clients transform their enterprise with real-time data and actionable insights that are simple to use at speed and at scale, without getting hung up on the challenges of implementing new technology and recruiting/retaining staff that are in high demand in the marketplace.

Following are key benefits of AIP:

- End-to-End Field-Tested Technology Solution: Full suite of solution components including analytics applications, visualization, analytics, storage, and data ingestion that is being used effectively at over 100 commercial clients today.
- Highly Scalable: Analytics and Big Data platforms must be scalable to meet current and future data retention needs and flexible in its solution components to meet changing needs. One of the solution benefits of why we are recommending the AIP is its cloud-based hosting. The cloud-based hosting provides participating entities with the flexibility to scale their analytics environment to the appropriate size based upon their data retention policies. The cloud-based solution also streamlines the solution component installation process.
- Flexible Commercial Pricing and Licensing: Pre-negotiated pricing and licensing are provided that will allow participating entities to have simple contracting, pay for only what you use, avoid large capital investment, scale as you grow, platform support, and the ability to turn solution components on and off.
- Automated Provisioning: participating entities would have the ability to create a working Big Data environment within a few days including users, security, network connections, firewall, and QA process.
- Recommended Practice Security: Security layers are provided that include network infrastructure, identity and access, application security, data security, and security event management and governance. Accenture takes data security very seriously and we will comply participating entities' data security standards and regulations to verify that data is protected both in static and in transition.
- Platform Support: Accenture provides support for the platform on a 24/7 basis.

The strength of AIP allows participating entities full access to all the solution components supported across the analytics stack of technologies. Participating entities are not limited to our recommended stack or anyone else's recommended solution stack. Participating entities can use the full suite of pre-negotiated software products or introduce their own custom solution components. As an example, if the participating entity typically uses Tableau for data visualization and then chooses to prototype similar capabilities in Qlik, Qlik can quickly be enabled within a few days in the state's instance of AIP for use by developers, selected vendors, and team members.

Accenture DevOps Platform

The Accenture DevOps Platform (ADOP) is a cloud-based development platform bringing together an integrated collection of enterprise and open source tools for developing, deploying, and managing applications using DevOps and ALM (Application Life Cycle Management) recommended practices.

The ADOP – Enterprise offerings and usage model is illustrated in Figure 6:

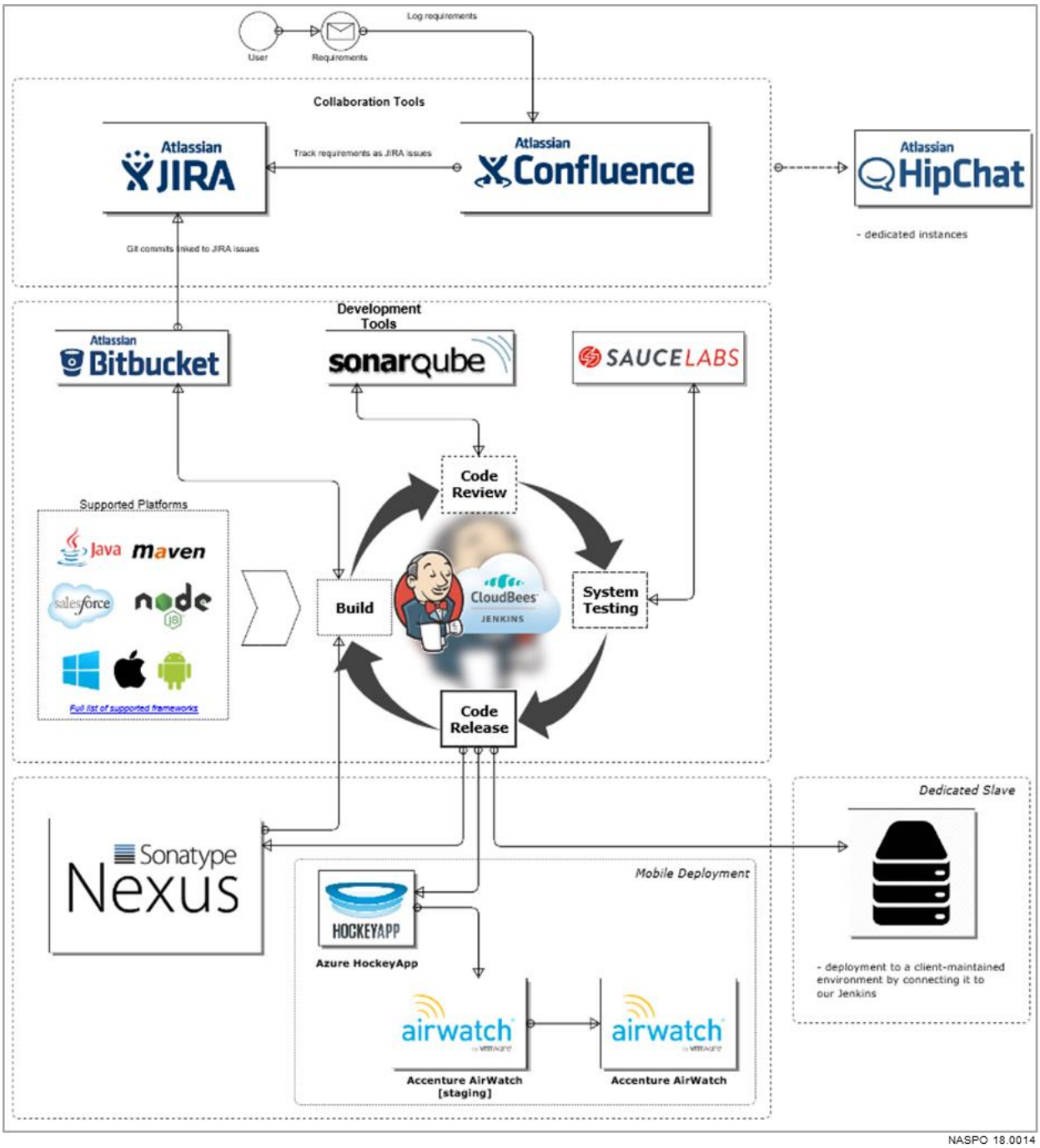


Figure 6. Architectural view of our ADOP Enterprise Offerings.

Accenture Virtual Assistant Platform

The Accenture Virtual Assistant Platform (AVAP) depicted in Figure 7, would provide participating entities a solution to augment worker capacity and transform service delivery by introducing cognitive services

and intelligent automation. End users of the platform may interact with the virtual assistants through a variety of channels including voice, online chat as well as SMS text messages. A service orchestration engine (SOE) is the centerpiece to integrate the natural language understanding capabilities of the Platform with robotic process automation (RPA). The Platform can understand the intent of a user request, and through the SOE, respond appropriately by either corresponding directly to the user, calling custom or commercial application program interfaces (APIs) or web services. Additionally, the Platform can be trained to effectively and accurately mimic worker procedures so that RPA processes complete automated actions in one or more systems.

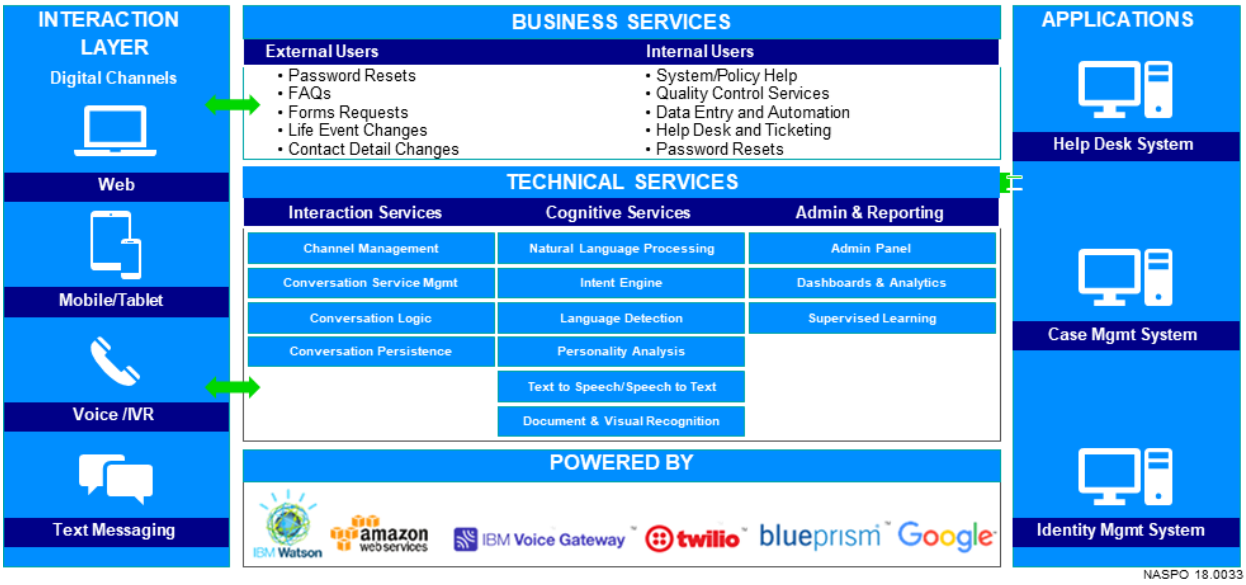


Figure 7. The AVAP offers a diverse stack of proven, industry-leading technologies to rapidly introduce a set of cognitive services and expand capabilities over time to transform service delivery.

To provide actionable insights and operational support for the primary offering, Accenture includes reporting capabilities and a system administration panel. The system administration panel and reporting capability includes access to real-time information on the health, configuration, and usage statistics of the solution.

Salesforce Service Cloud

Salesforce Service Cloud is the industry leading customer relationship management (CRM) engagement center solution. It will provide a 360-degree view of your customer and will provide your organization call center representatives with the resources they need to deliver superior customer experiences.

With the Salesforce Service Cloud, illustrated in Figure 8, your organization's service and support personnel can achieve more 1st call resolutions, better maintain SLAs, and increase customer satisfaction ratings at a fraction of the cost. Your organization can collect customer support requests from all channels, automate routine processes, and open up knowledge base and FAQ's via your website.

Salesforce's powerful analytics engine can also deliver key performance metrics tailored to government organizations fast, without the need for code or IT resources. Used in call centers across all levels of government and in nearly every industry, Salesforce helps deliver great service with 28% improved agent productivity, 22% decrease in support costs, 31% faster case resolution, and 35% increase in customer satisfaction. What's more, with the power of the Salesforce Lightning Platform, Salesforce Service Cloud can be quickly and easily extended, customized, and adapted to any customer service challenge.

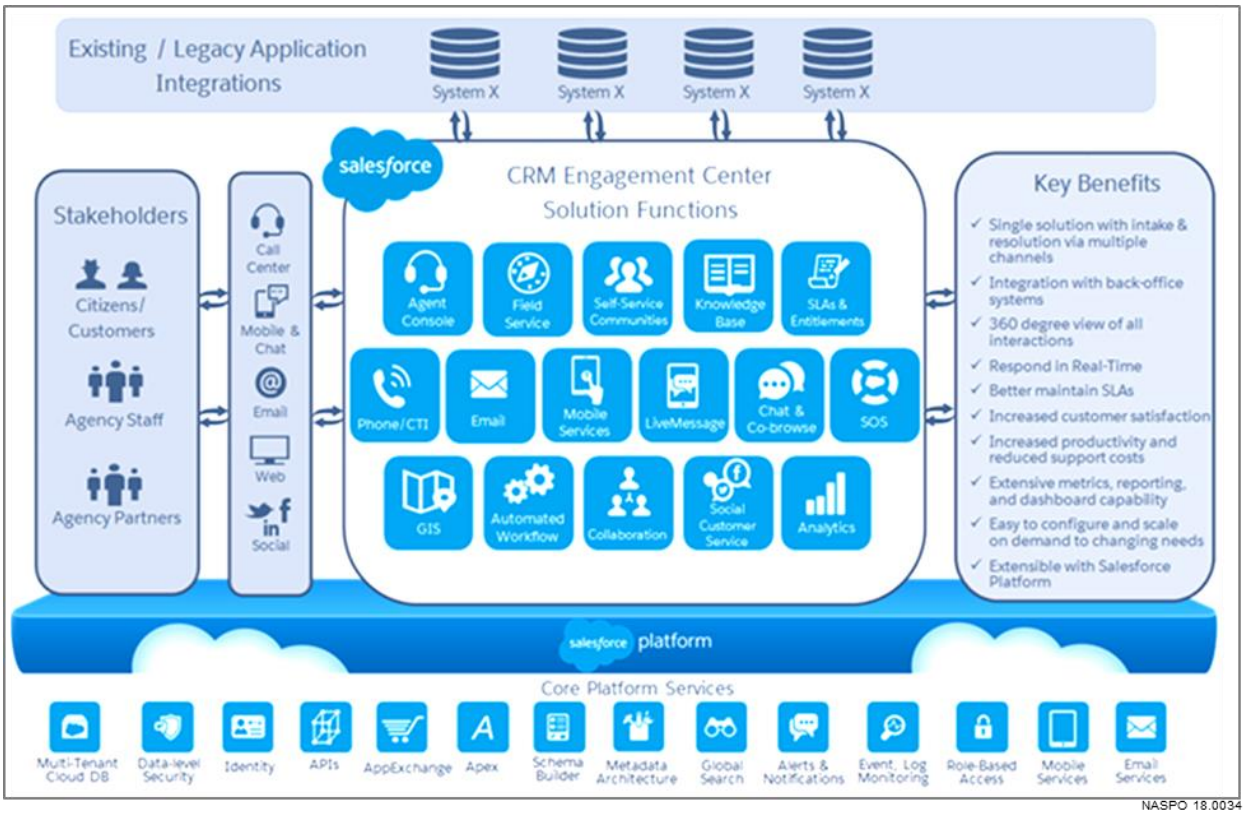


Figure 8. Accenture's Cloud First team delivers value to our clients by implementing scalable cloud solutions with the Salesforce CRM.

Accenture is Salesforce's largest integrator and its #1 Alliance Partner. Accenture Cloud First Applications help you reach your desired end state by enabling your capabilities, people, processes and skills to harness the true power of cloud application platforms and their innovative multitenancy ecosystem, at every stage of your cloud journey. Accenture delivers high quality, high performing Salesforce functionality through our specialized Salesforce workforce, deep-industry skills and delivery capabilities.

8.1 (M)(E) TECHNICAL REQUIREMENTS

8.1.1 - 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 characteristics defined in NIST Special Publication 800-145.

ON-DEMAND SELF-SERVICE

NIST characterizes On-Demand Self-Service as the ability for consumers to unilaterally and automatically provision computing capabilities to include server time and network storage without manual intervention for each service. Accenture understands that self-service of IT resources is a compelling reason to use the cloud as it allows organizations to quickly provision IT resources. Accenture is offering several IaaS, PaaS, and SaaS solutions that comply with this NIST Characteristic. Below is a description of how Amazon Web Services (AWS) and Salesforce meet this characteristic. Accenture cloud solutions built on AWS meet this characteristic by leveraging the AWS platform.

AWS provides customers of all sizes with on-demand access to a wide range of cloud infrastructure services, charging you only for the resources you use. AWS enables you to eliminate the need for costly hardware and the administrative pain that goes along with owning and operating it. Instead of the weeks and months it takes to plan, budget, procure, set up, deploy, operate, and hire for a new project, our customers can simply sign up for AWS and immediately begin deployment in the cloud with the equivalent of 1, 10, 100, or 1,000 servers. Whether an organization needs to prototype an application or host a production solution, AWS makes it simple for customers to get started and be productive.

Salesforce PaaS and SaaS solutions are delivered on-demand via the web and can be accessed with a browser and internet connection or mobile device. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up customers to manage their mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE). No installations on users' laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.

BROAD NETWORK ACCESS

NIST characterizes Broad Network Access as services that are available over a network and accessed through standard mechanisms that encourage the use of heterogeneous platforms. Accenture understands that this independence from geography and deployment of services that are easily network accessible allows for flexibility in deploying, connecting, and accessing IT resources. Accenture is offering several IaaS, PaaS, and SaaS solutions that comply with this NIST Characteristic. Below is a description of how Amazon Web Services (AWS) and Salesforce meet this characteristic. Accenture cloud solutions built on AWS meet this characteristic by leveraging the AWS platform.

AWS provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. Cloud computing providers such as AWS own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application.

RESOURCES POOLING

NIST characterizes Resources Pooling as services that "the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand." Accenture understands the significance of resource pooling to participating entities as it verifies greater efficiency in IT services and

provides for economies of scale in pricing. Accenture is offering several IaaS, PaaS, and SaaS solutions that comply with this NIST Characteristic. Below is a description of how Amazon Web Services (AWS) and Salesforce meet this characteristic. Accenture cloud solutions built on AWS meet this characteristic by leveraging the AWS platform.

The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate customers from each other. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS Security Standards 3.2 as of July 2016.

Salesforce is a multitenant cloud-based subscription service. Multi-tenant cloud solutions provide a single, shared infrastructure, one code base, one platform that is all centrally managed, with platform-based API to support all integration traffic, and multiple release upgrades included as part of the subscription service. Multi-tenancy and the Cloud Computing model remove unneeded tasks from the process of delivering, managing, and integrating software. Salesforce customers will not need to maintain any hardware or software. Without multiple versions to support, integrations don't break during updates; they are simply updated automatically. As a result, both the initial integration and its continued maintenance are simplified. More resources can be focused on creating a better product, with a faster cycle of innovation, instead of having to manage the complexity of many different versions to support a vast installed base.

RAPID ELASTICITY

NIST specifies that for Rapid Elasticity, resources should be provisioned and released elastically and may also be required for automated scalability to meet rapid outward and inward demands. Accenture believes that rapid elasticity provided through the cloud allows clients to quickly scale up or down as needed to meet demand and only pay for resources that are needed at that moment in time. Accenture is offering several IaaS, PaaS, and SaaS solutions that comply with this NIST Characteristic. Below is a description of how Amazon Web Services (AWS) and Salesforce meet this characteristic. Accenture cloud solutions built on AWS meet this characteristic by leveraging the AWS platform.

AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications, instantly scale up as your workload grows, and instantly scale down based on demand. Customers need to be confident that their existing infrastructure can handle a spike in traffic and that the spike will not interfere with normal business operations. Elastic Load Balancing and Auto Scaling can automatically scale a customer's AWS resources up to meet unexpected demand and then scale those resources down as demand decreases.

Salesforce PaaS and SaaS solutions are built on shared resources with extra underlying capacity that can quickly be provisioned for a customer. Salesforce does not require customer intervention to scale, but instead automatically provisions additional capacity if needed in a rapid manner.

MEASURED SERVICE

NIST requires that cloud providers allow for resource control and optimization through metering capabilities like a pay-per-use or charge-per-use basis. Accenture understands the importance of measuring services to adequately forecast spend and allow for purchasing entities to control use of IT resources. Driven primarily by this characteristic, Accenture created the Accenture Cloud Platform (ACP) to help customers better understand where their cloud spend was occurring. ACP includes the capability to aggregate cloud spend across cloud providers to furnish the business with a single view of cloud spend. ACP is now the leading Cloud Management Platform according to Gartner and we are excited to bring this capability to participating entities.

This includes measurements on amount of storage allocated, CPU resources used, and amount of memory used for IaaS services. PaaS services are usually measured and billed based on number of requests handled, number and size of objects, or number of CPU cycles combined with memory size for a function invocation. SaaS models typically are measured and billed based on the number of users in a given month.

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

Accenture is willing to comply with the requirements of Attachments C&D. We are offering solutions that comply with the NIST descriptions of Cloud Service models, including IaaS, PaaS, and SaaS solutions. We can support the following risk categories: Low, Moderate, and High. Our solutions are primarily served through Public cloud models, but can support private, community, and hybrid cloud deployments in some cases. Our services can be sub-categorized according to NIST terminology as shown below.

Accenture is offering the following IaaS services:

- Computer/Infrastructure Services
  - Accenture Cloud Platform (ACP)
- PC/Desktop "as a service"
  - Desktop as a Service (DaaS)

Accenture is offering the following PaaS services:

- Database
  - Database as a Service (DBaaS)
- Development, Testing and Deployment
  - Accenture Reach Platform
  - Salesforce Platform

Accenture is offering the following SaaS services:

- Analytics
  - Accenture Insights Platform (AIP)
- Cloud and Infrastructure Management Tools

  - Accenture DevOps Platform (ADOP)
- Customer Relationship Management
  - Salesforce CRM
- Other - Chatbots
  - Accenture Virtual Assistant Platform (AVAP)

8.1.3 - 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.

Accenture is prepared to provide participating entities with cloud-based services through AWS and Salesforce. Accenture has extensive experience customizing cloud architectures for public and private entities that adhere to the services definitions and deployment models identified in this RFP. See section 8.1.1 for information on how our offerings meet the five essential characteristics found in NIST Special Publication 800-145.

Accenture's cloud solutions fit into multiple categories described in Attachment D. AWS and Salesforce are public cloud providers that can support a customer's hybrid cloud environment. Accenture's solutions such as the Accenture Insight's Platform are primarily provided through public cloud, but can be leveraged in a private or hybrid cloud environment as well.

Our solutions can be categorized by service model (e.g., IaaS, PaaS, SaaS) with subcategories as described in our response to 8.1.2. Accenture's approach provides managed cloud services that are measured, scalable, and available on-demand with support for self service delivery over the network.

8.2 (E) SUBCONTRACTORS

8.2.1 - 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. Subcontractors do not need to comply with Section 6.3.

Accenture is excited to bring IaaS, PaaS, and SaaS to purchasing entities through highly qualified subcontractors. As a global technology services firm, Accenture has deep partnerships with many of the leading cloud providers. In addition to these partners, Accenture is exploring relationships with additional cloud service providers to bring an even more robust set of cloud services to our customers.

Accenture is proposing to provide services directly and through subcontractors as follows:

SERVICE MODEL	RESPONSE
IaaS	Amazon Web Services
PaaS	Amazon Web Services, Salesforce
SaaS	Amazon Web Services, Salesforce, IBM Cloud, Google Cloud, Twilio

Below is more information about the relationships with each of our subcontractors.

AMAZON WEB SERVICES

In 2006, Amazon Web Services (AWS) began offering IT infrastructure services to businesses in the form of web services -- now commonly known as cloud computing. One of the key benefits of cloud computing is the opportunity to replace up-front capital infrastructure expenses with low variable costs that scale with your business. With the Cloud, businesses no longer need to plan for and procure servers and other IT infrastructure weeks or months in advance. Instead, they can instantly spin up hundreds or thousands of servers in minutes and deliver results faster.

Today, Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia, customers across all industries and governments are taking advantage of their platform.

Accenture and AWS have been collaborating for nearly twelve years to bring cloud solutions to our customers through the Accenture Amazon Business Group (AABG). AABG combines the resources, technical expertise and industry knowledge of Accenture and AWS, all through a single point of contact. As a result, it enables enterprises to accelerate their strategies to realize ongoing business value from cloud adoption and transformation.

Uniquely, this decade-long collaboration can support clients end-to-end: from strategy ideation, to migration, to operation and run, securely and at scale all powered by AABG's joint investments in world-class accelerators, centers of excellence and digital skills.

SALESFORCE

Accenture is the go-to provider for companies looking to configure and deploy cloud solutions that enable high performance. We apply field-tested methodologies and tools to simplify—and accelerate—complex, global Salesforce implementations. Above all, we help our clients realize the value of the cloud in many areas of their operations—from sales to customer service and support.

Salesforce is the world leader in customer relationship management software. Its cloud, social, and mobile solutions cover sales, service and marketing, workplace collaboration, and performance management. Additionally, its Force.com® cloud platform enables businesses to take advantage of platform as a service (PaaS) efficiencies and run complete enterprise resource planning solutions and custom applications.

As market leaders in our respective industries, we have established a strong, dynamic, client-centered partnership that is shaping the future of cloud computing. For nearly 10 years, we have partnered to deliver business value and strategically invested in innovative technology and client-centered alliance initiatives. Along the way, we have helped hundreds of organizations achieve the full potential of enterprise cloud computing.

IBM CLOUD

IBM Partner World is a global marketing and enablement program for IBM Business Partners. Accenture is a Platinum Level Business Partner, and does more work with IBM Technology than any other global systems integrator. As a Platinum Level business partner, Accenture gains privileged insight into IBM product engineering, R&D, and future roadmaps, ensuring we have the insight to guide our clients toward a sustainable solution using the right technology delivered with the highest quality. The engine for this partnership is the Accenture Center for IBM Technologies (ACIT), employing more than 650 full-time solution architects.

The IBM Cloud offers over 170 services ranging from bare metal, containers, and serverless computing to hyper scale infrastructure, blockchain and Artificial Intelligence, all with built in security at their core. The multitude of services offered allows organizations to focus on enterprise innovation, make better sense of their data, infuse cognitive capabilities, and tap into industry and technology expertise.

The 20+ year alliance between Accenture and IBM has resulted in the support of over 1,200 concurrent client engagements with over 10,000 assets utilized annually. The active collaboration with IBM has allowed Accenture to deliver significant client value through innovative solutions

GOOGLE CLOUD

Accenture's partnership with Google is helping organizations solve today's greatest challenges by combining the power of Google Cloud technology and Accenture's industry expertise and global delivery capabilities. From providing solutions with machine learning for smarter, more personalized experiences to rearchitecting infrastructure and workforces with virtual assistants for more agile, data-driven intelligent processes and unparalleled collaboration, the Accenture and Google partnership is driving new levels of business and IT transformation.

TWILIO

Twilio is a cloud communication platform for building SMS, Voice & Messaging applications on an API built for global scale. Twilio offers a variety of products and solutions which allows organizations to increase engagement with customers, shorten coordination time by connecting users at the right moment, and improve customer satisfaction by building omni-channel contact centers.

8.2.2 - 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.

Accenture would use subcontracts to provide the IaaS, PaaS, and SaaS services and Accenture services. Accenture will work with the subcontractors to provide these services and solutions to participating entities. Subcontractors would be vetted to ensure they have the necessary qualifications to do business within the State of Utah and any participating entities. Subcontractors would also comply with the applicable terms and conditions of the RFP and subsequent contract, as well as all Participating Addendums for the States they are subcontracting in. Refer to 8.2.1 for more information on each subcontractor's services.

8.2.3 - 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.

See section 8.2.1 for information on each of our subcontractor's services and qualifications. Accenture would confirm a subcontractor has the necessary certifications to do business in the state before adding them to the contract as a subcontractor. Accenture already has extensive partnerships with our subcontractors, but would put a specific agreement in place with the subcontractor to ensure optimal efficiency with the subcontractor's responsibilities for this contract.

8.3 (E) WORKING WITH PURCHASING ENTITIES

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."

Our Information Security team works to preserve information integrity and confidentiality in a world of ever-advancing threats, regulations, expectations, and technical capabilities. We maintain formal governance relationships with Accenture's Legal, Data Privacy and Business Continuity functions. The team also works closely with Accenture's Security practice to ensure that our clients benefit from our internal knowledge and experience. Strong relationships are maintained with law enforcement agencies, third-party specialist advisors, and the information security organizations of clients and suppliers.

If an Accenture employee suspects a data breach, they are trained to immediately escalate to their manager and up their leadership chain if their immediate manager is not available. If it is determined that a data breach is likely, the project team would immediately notify our contact with the participating entities. We also involve our central Accenture Security Operations Center (ASOC), which has the ability to pull in security SMEs and data analysts to study the issue and determine appropriate escalation and resolution paths. Our goal is to keep all impacted parties aware of the current status of the issue including the total impact and scope of the breach. This communication process would be determined in conjunction with the client, but usually involves a daily call or email to keep responsible parties updated on the issue.

After the breach is resolved, our ASOC team remains involved to lead the effort to remediate the source of the issue and work with the customer to determine appropriate notifications to individuals whose data was breached. Accenture continuously works to improve the security of our delivery to customers through training, improved tools, tracking of engagement's compliance to our security controls, and regular communications emphasizing the importance of security to our work. We strive to continue to improve our security and maintain ISO27001 certification from BSI.

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.

Accenture asserts that we will not engage in, nor permit agents to push adware, software, or marketing that is not explicitly authorized by the participating entity or in the Master Agreement.

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

Accenture proposes the implementation of virtual private cloud environments to provide user test/staging environments that are identical to production. Virtual private cloud environments offer both the computing resources and isolation required for the Purchasing Entities to manage the design, engineering, and implementation of their cloud-based solutions.

The virtual private cloud environments provided by our proposed public cloud providers include the following characteristics:

- Provision logically isolated computing/processing resources to host application-hosting environments
- Configuration templates that can be used to verify that environments are identical
- Configuration templates that can be used to quickly create new environments
- Controlled access to virtual private cloud that can help to separate environments and users accessing environments

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

The web sites and user interfaces proposed would comply with a participating entity's accessibility policy and the Americans with Disability Act as applicable and are accessible to people using assistive technologies.

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 a minimum.

All cloud offerings proposed by Accenture are accessible using current released versions of multiple browser platforms such as Internet Explorer, Firefox, Chrome, and Safari.

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.

Accenture would work with participating entity and cooperate while shaping a specific statement of work to determine whether any sensitive or personal information will be involved in the project. The key personnel identified for this contract would initiate these discussions either in person or through a conference call to make the determination. Accenture has significant experience working with government agencies and is committed to providing services that are secure for our customers.

8.3.7 - Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Accenture uses the Integrated Project plan to look at the program in the big picture. The integrated schedule has task items, start date, end date, assigned person, risks, and status. The Work Plan or Integrated schedule is used to track development, testing, production live, and post-live activities and progress. Accenture would track program status and share updates (e.g., weekly, monthly) with the purchasing entities as defined in the statement of work.

8.3.8 - The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:
• How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.
• How Offeror will maintain discounts at the levels set forth in the contract.
• How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.
• How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change."

Accenture's proposed method of providing cloud services to participating entities includes services that are constantly being updated by our proposed vendors. Our approach is to provide all IaaS, PaaS, and SaaS services from these vendors with a consistent discount percentage across the services. Therefore, any technology changes or discounts implemented by these providers will be immediately available to our NASPO customers. We intend to update our official offering descriptions quarterly with any significant changes. In the event that a participating entity is negatively impacted by a service change and desires to transition that service, Accenture would enable the participating entity to make the transition through self-service or offer value added services to make the transition.

8.4 (E) CUSTOMER SERVICE

8.4.1 - Offeror must describe how it will ensure 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). "

Each Accenture engagement goes through a regular Quality Assurance Review process usually on a quarterly basis where an assigned QA reviewer works with the project team to confirm we are meeting our client's expectations. The QA Director works with the CAL to resolve any issues that are discovered during the QA Review.

Accenture also works to set up regular steering committee meetings that include the Project Director and the CAL. We use these meetings to confirm that we are meeting our client's expectations and to bring forth ideas on how we can improve our service in this ever-changing technology environment. Given that SLAs are established for each engagement, Accenture uses these meetings to discuss any SLAs that are of concern for either Accenture or our client.

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."

Accenture intends to comply with the requested customer service requirements as follows:

a) A lead representative will be assigned to each entity that executes a Participating Addendum. Accenture will keep the contact information current as requested.

b) This contact will be available via phone or email 7 am to 6 pm Monday through Sunday. At times when the contact is not available, Accenture will provide an alternate contact.

c) Accenture's representative will respond to email or phone inquiries within one business day.

d) Design services for the components that Accenture is offering are available through this our proposed offering. It is Accenture's experience that migrations to cloud environments are most successful when we take a structured approach including an assessment of the current environment followed by the development of a roadmap and strategy. Accenture would provide these services as described in our Value-Added Services and priced according to the scale of the customer's needs.

e) Installation services are included in the pricing for a number of the solutions that Accenture is offering. For many of our IaaS and PaaS offerings, there is no installation, but rather an implementation of the customer's specific workloads in the cloud environment. Accenture has provided a listing of value added services to assist customers with migrating applications and servers to our cloud offerings.

8.5 (E) SECURITY OF INFORMATION

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 the cloud service providers that we are proposing have strong security controls in place. For example, see below how AWS and Salesforce meet these requirements. Accenture specific cloud offerings built on AWS benefit from the underlying security that AWS provides.

AWS SECURITY

AWS Data Center Security

AWS does not disclose the exact location of its data centers and does not allow data center access to customers as this exposes a wide range of customers to physical access of a third-party. Instead of allowing customers to perform physical audits, AWS has an independent third-party perform audits of its data centers. These audits are conducted in accordance with the Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. The auditors produce a System and Organization Controls 1 (SOC 1), Type 2 Report in connection with the audit. Independent reviews of data center physical security are also part of an ISO 27001 audit, a Payment Card Industry (PCI) Data Security Standard (DSS) assessment, and an International Traffic in Arms Regulations (ITAR) audit.

AWS Physical and Environmental Security

AWS's data centers are state of the art, using innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS Cloud. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff using video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

AWS Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system uses smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

AWS Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

AWS Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

AWS Management

AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

AWS Storage Device Decommissioning

As part of AWS's storage decommissioning process, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.

AWS will provide the SOC 1 Report to customers under NDA. The AWS Security Center provides up-to-date information on AWS audits by independent third-party auditors.

SALESFORCE SECURITY

Salesforce understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and its own success. Salesforce uses a multi-layered approach to protect that key information, constantly monitoring and improving application, systems, and processes to meet the growing demands and challenges of security.

Independent audits confirm that its security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce gives you the peace of mind only a world-class security infrastructure can provide.

Salesforce Third-Party Validation

Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, Salesforce continually seeks relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by a third-party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.

Salesforce protection at the application level

Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.

Salesforce protection at the facilities level

Salesforce security standards are stringent and designed with demanding customers in mind, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk or tape. These backups provide a second level of physical protection. Neither disks nor tapes ever leave the data center.

Salesforce protection at the network level

Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find:

- Live and historical data on system performance
- Up-to-the minute information on planned maintenance
- Phishing, malicious software, and social engineering threats
- Best security practices for your organization
- Information on how we safeguard your data

Accenture understands that security requirements vary greatly even within different units of a government agency and will leverage the recommended cloud solution for a given customer's needs. This applies to determining the methods by which Accenture would hold, protect, and dispose of data following the completion of any contract services.

Accenture's cloud vendors all have strong security standards and practices in place to protect customer data from breaches.

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

Accenture would support and comply with any regulations or sensitive data compliance needs that the customer identifies. The solutions that Accenture is proposing have the ability to limit customer information to a secure and isolated environment if needed. Under no circumstances would Accenture ever publish or release secure customer data.

8.5.3 - 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.

Accenture's approach for providing cloud services enables the Purchasing Entity as the owners of the user accounts and data. Therefore, Accenture would only access that information if specifically required for the statement of work with the Purchasing Entity and with that entity's permission. Under no circumstances will Accenture or its cloud partners release protected information without expressed customer consent and direction.

8.6 (E) PRIVACY AND SECURITY

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.

Accenture is committed to providing secure solutions that protect the data of our customers. The cloud providers that we are partnering with and Accenture's own cloud solutions provide the capability to help meet a variety of Privacy and Security requirements. Accenture would work with the Participating Entities to define the right solution based on their requirements including the risk level of the data as described in Attachment D. An example of the specific solution capabilities is highlighted below with the Salesforce compliance to these requirements.

On May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4.

Salesforce provides contractual assurance to its customers that the Customer Data hosted in Salesforce's services will be kept confidential and not accessed by third parties except under narrow circumstances (such as a customer support issue or as required by law). In the case of customer support, the company's personnel will access a customer's Org only with prior approval and subject to confidentiality obligations.

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.

Accenture's IaaS, PaaS, and SaaS offerings include solutions built on AWS and the ability to offer AWS and Salesforce directly. Below are the certifications that AWS and Salesforce hold.

AWS

AWS Compliance enables customers to understand the robust controls in place at AWS that facilitate security and data protection in the cloud. The AWS Cloud infrastructure has been designed and is managed in alignment with the following regulations, standards, and recommended practices:

- Federal Risk and Authorization Management Program (FedRAMP)
- System and Organization Controls (SOC) 1, SOC 2, and SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001
- Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6
- Federal Information Security Management Act (FISMA)
- US Health Insurance Portability and Accountability Act (HIPAA)
- FBI Criminal Justice Information Services (CJIS)
- National Institute of Standards and Technology (NIST) 800-171
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
- Family Educational Rights and Privacy Act (FERPA)
- Information Security Registered Assessors Program (IRAP) (Australia)
- IT-Grundschutz (Germany)

For information on all the security regulations and standards with which AWS complies, visit the AWS Compliance page.

Compliance is a Shared Responsibility

Because AWS and its customers share control over the IT environment, both parties have responsibility for managing the IT environment. AWS's part in this shared responsibility model includes providing its services on a highly secure and controlled cloud and providing a wide array of security features that customers can use. Conversely, customers are responsible for configuring their IT environments in a secure and controlled manner for their purposes.

The customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation, and verification of IT controls. AWS can help relieve the customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS, which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as

required. AWS customers are required to continue to maintain adequate governance over the entire IT control environment regardless of how IT is deployed.

Resources for Maintaining Compliance

AWS has published several whitepapers to assist their customers in learning more about and complying with their standards and assurance programs. These whitepapers also provide recommended practices for overall governance and security in the cloud. The *AWS: Risk and Compliance* and *Automating Governance: A Managed Service Approach to Security and Compliance on AWS* whitepapers are especially helpful.

In addition, AWS provides several Compliance Enablers to help customers establish and operate their cloud resources in a secure, controlled, and compliant environment. These workbooks, whitepapers, and matrices are meant to help customers understand AWS-specific compliance processes and to guide them with adherence to compliance requirements while using AWS Cloud resources.

SALESFORCE

Salesforce and the Salesforce Force platform is ISO 27001 certified and PCI-DSS compliant. SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include:

- FedRAMP Authority to Operate from Department of Health and Human Services
- CSA 'Consensus Assessments Initiative'
- JIPDC (Japan Privacy Seal)
- Tuv (Germany Privacy Mark)
- TRUSTe
- HIPAA

In provisioning and operating the services, Salesforce complies with the provisions of HIPAA's Privacy Rule and Security and the HITECH Act that are applicable to business associates. Salesforce's customers are still responsible for complying with the same in their capacity as a covered entity or business associate using the Salesforce services. The services' features permit customers to customize use as per a compliance program for HIPAA (including the HITECH Act) and many customers store protected health information (PHI) on our service. From a legal standpoint, some of our customers have asked Salesforce to assist them in meeting their compliance obligations; for example, by entering into business associate agreements (BAA) to address formal legal requirements pertaining to use and disclosure of protected health information (PHI).

FERPA

Salesforce maintains appropriate administrative, physical, and technical safeguards to help protect the security, confidentiality, and integrity of data our customers submit to the Salesforce Services as Customer Data. Salesforce's customers are responsible for ensuring the security of their Customer Data in their use of the service and implementing any necessary customer-controlled settings. To aid,

Salesforce offers robust security functionality that provides our customers the flexibility to use the application in a configuration that furthers compliance with local data protection laws and regulations.

While Salesforce complies with applicable laws in provisioning and operating the Salesforce services, it is the sole responsibility of Salesforce's customers to ensure compliance with applicable laws in their respective uses of the Salesforce services. PCI-DSS Salesforce is PCI Level 1 compliant and has received a signed Attestation of Compliance (AoC) for the Payment Card Industry Data Security Standard (PCI-DSS). Salesforce customers who must adhere to PCI compliance may store personal account numbers ("PAN" or "credit card numbers") in Salesforce, with the following caveats:

- PANs may only be stored in a custom field encrypted via Classic Encryption or supported field types via the Platform Encryption functionality. PANs must not be stored in clear text fields, attached files, or any other location.
- Refer to the Help & Training portal for information on supported fields which can be encrypted using Platform Encryption: https://help.salesforce.com/HTViewHelpDoc?id=security_pe_overview_fields.htm&language=en_US
- Customer administrators must configure Salesforce features to support their organization's PCI controls. NIST SP 800-171NIST Special Publication 800-171 is intended for use by federal agencies when agencies are providing CUI to nonfederal organizations (or when CUI is developed by those organizations for federal agencies) for purposes unrelated to information processing. In other words, the nonfederal organizations are not operating their information systems to process agency data, including CUI, on behalf of the agency but rather for other purposes (e.g., when designing or producing an aircraft, performing a study, or conducting background investigations for security clearances).

Salesforce recommends that its customers use the classifications as detailed in FIPS 199:

http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

FIPS 140-2, FIPS 197, FIPS 199, and FIPS 200

On May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4.

As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2/3 cryptographic implementations for data being transferred between the customer's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data.

Additional information is provided below.

Data Transmission between the customer's web browser and Salesforce:

Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048-bit Public Key. Our service uses International/Global Step Up certificates. We support one-way TLS, in which customers create secure connections before sharing private data. Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary.

Data Transmission for Backup Media:

Media containing customer data is not transported outside of controlled salesforce.com areas and therefore relies on physical access controls to protect the data.

Data at Rest:

NIST 800-53 Rev. 3 states in SC-28, “Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system.” SC-28 also states, “Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.” All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce's secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data.

Primary Data Storage:

User passwords are stored in the RDBMS encrypted via the SHA algorithm with a 256-bit hash. This is a one-way hash. The passwords are encrypted by the application.

For primary data storage, Salesforce provides customers with a built-in capability to apply field-level encryption, using 128-bit keys with Advanced Encryption Standard (AES) encryption (as defined by FIPS 197), for a selection of custom fields included in the Salesforce Platform and CRM applications. Field-level encryption ensures the data associated with designated fields is encrypted in storage. Additional information regarding field-level security can be accessed via the following link:

https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_about_encrypted_fields.htm&language=en

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.

Through Accenture’s Client Data Protection (CDP) program, we establish controls that effectively secure data from both internal and external threats. We also restrict access to data to minimize the possibility of exposure to unauthorized personnel. Our controls include active management of privileged accounts such as Database Administrators that would have access to stored data. Laptops and mobile devices have multiple security controls including hard disk encryption on laptop, device encryption on mobile devices, and web content filtering. In addition to these controls that Accenture implements for our people, we leverage the data protection capabilities of our public cloud providers. The following sections discuss the

AWS capabilities that apply to Accenture's cloud offerings built on AWS on and directly to our AWS offering. We have also included information on how Salesforce meets this requirement.

AWS

The AWS virtual infrastructure is designed to provide optimum availability while confirming customer security, privacy, and segregation. With the AWS Cloud, not only are infrastructure headaches removed, but so are many of the security issues that come with them. 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. Their environmental systems are designed to minimize the impact of disruptions to operations, and their 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 their 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 using 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 propose security recommended practices, such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.

SALESFORCE

Salesforce understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce Force.com gives you the peace of mind only a world-class security infrastructure can provide.

Protection at the application level

Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.

Protection at the facilities level

Salesforce security standards are stringent and designed with demanding customers in mind, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk or tape. These backups provide a second level of physical protection. Neither disks nor tapes ever leave the data center.

Protection at the network level

Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

Secure Data Centers

Data centers provide only power, environmental controls, and physical security. Salesforce employees manage all other aspects of the service at the data centers. Colocation data center personnel do not have network or logon access to the Salesforce systems. Colocation personnel have physical access to the Salesforce secure server room in the event of an emergency, but do not have keys to the individual racks containing hardware. Data centers maintain a common baseline of physical and environmental controls across data centers.

The exterior perimeter of each anonymous data center building is bullet resistant, has concrete vehicle barriers, closed-circuit television coverage, alarm systems, and manned 24/7 guard stations that together help defend against non-entrance attack points. Inside each building, multiple biometric scans and guards limit access through interior doors and to the Salesforce secure rooms at all times.

Access to Salesforce's secure server rooms in the datacenter is authorized based on position or role. Additional access controls enforced by an electronic key box are implemented for the dedicated Salesforce Government Cloud racks to ensure that access is limited to Qualified U.S. Citizens. Salesforce has an established process to review data center access logs to the server room. Additionally, an at least annual assessment of the data center is performed to ensure the data centers are meeting Salesforce's security control requirements.

In addition to securing the data center locations, it is critical that the data center facilities maintain robust critical infrastructure to support Salesforce through the following services:

Temperature and Humidity Controls

- Humidity and temperature control
- Redundant (N+1) cooling system

Power

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

Secure Network Logistics

- Concrete vaults for fiber entry
- Redundant internal networks
- Network neutral; connects to all major carriers and located near major Internet hubs
- High bandwidth capacity

Fire Detection and Suppression

- VESDA (very early smoke detection apparatus)
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

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).

Through Accenture's Client Data Protection (CDP) program, we establish controls that effectively secure data from both internal and external threats. We also restrict access to data to minimize the possibility of exposure to unauthorized personnel. Our controls include active management of privileged accounts such as Database Administrators that would have access to stored data. Laptops and mobile devices have multiple security controls including hard disk encryption on laptop, device encryption on mobile devices, and web content filtering. In addition to these controls that Accenture implements for our people, we leverage the data protection capabilities of our public cloud providers. The following sections discuss the AWS capabilities that apply to Accenture's cloud offerings built on AWS on and directly to our AWS offering. We have also included information on how Salesforce meets this requirement.

AWS

Not only are applications and data protected by highly secure facilities and infrastructure, they are also protected by extensive network and security monitoring systems. AWS and their partners provide tools and services that can help customers every step of the way to verify understanding of and transition to a secure cloud. 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. The following are included in the AWS-provided security features:

- **Managed DDoS Protection:** AWS Shield is a managed DDoS protection service that provides always-on detection and automatic inline mitigations that minimize downtime and latency. With two tiers to choose from—Standard and Advanced—customers can protect multiple layers of their web applications against DDoS attacks.

- **Machine Learning-powered Security:** Amazon Macie is a full managed security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides dashboards and alerts that give visibility into how this data is being accessed or moved.
- **Managed Threat Detection:** Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers.
- **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 Sockets 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. When instances reside within an Amazon Virtual Private Cloud (Amazon VPC) subnet, customers can control egress and 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 IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security recommended practices of role separation and least privilege.
- **Multi-Factor Authentication (MFA):** AWS provides built-in support for MFA for use with AWS accounts and individual 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 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 use 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.

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.

- **AWS Personal Health Dashboard:** AWS Personal Health Dashboard provides a personalized view into the performance and availability of the AWS Cloud services you are using and alerts that are automatically triggered by changes in the health of those services. In addition to event-based alerts, Personal Health Dashboard provides proactive notifications of scheduled activities, such as any changes to the infrastructure powering your resources, enabling you to better plan for events that may affect you.
- **AWS Trusted Advisor:** Provided automatically when AWS customers sign up for AWS 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, Amazon RDS DB instances, 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 their AWS resources and view the configuration of each. Customers can receive notifications each time a configuration changes and dig into the configuration history to perform incident analysis.
- **Amazon Inspector:** Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector

automatically assesses applications for vulnerabilities or deviations from recommended practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

- **Amazon Macie:** Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as Personally Identifiable Information (PII) or intellectual property and provides dashboards and alerts that give visibility into how this data is being accessed or moved.
- **AWS Organizations:** AWS Organizations allows you to create groups of AWS accounts that you can use to more easily manage security and automation settings. With AWS Organizations, you can centrally manage multiple accounts to help you scale. You can control which AWS Cloud services are available to individual accounts, automate new account creation, and simplify billing.

More information on these and other features is available at http://aws.amazon.com/security/aws-security-features/.

SALESFORCE

Salesforce provides contractual assurance to its customers that the data hosted in the Salesforce Services will be kept confidential and not accessed except under narrow circumstances (such as a support issue) and only for a set amount of time chosen by customer. In such circumstances, we will access your org only with prior approval and subject to a Non-Disclosure Agreement (NDA).

To protect against access through the application, Salesforce employees don't have access at the application level for any customers, unless the customer grants access through the “login as” feature.

Access to the production environment infrastructure is restricted to a very limited number of full-time Salesforce employees required to manage the service. Salesforce's Technical Operations team and Release Managers have logical access to servers. These employees must authenticate to the production environment via a secure server (Secure Global Desktop) using 2 points of RSA two-factor authentication. This tool provides pixel data only to these administrators. Systems access is role-based and controlled and logged. DBAs do not have login access to customer's instances (org) and do not see customer data in an assembled manner. They manage the system in aggregate-performance tuning, allocating space, building indices, etc. The Oracle tables and rows in our infrastructure do not reflect the view of a single customer instance (org) since we are multi-tenant and the data is spread across multiple disk arrays.

Database administrator account activity is logged. These logs are sent to the security information and event management (SIEM) system. These database activities logs are reviewed for appropriateness by the Computer Security Incident Response Team (CSIRT) team on a regular basis. This log data is also available as a forensic audit trail to support CSIRT during incident investigations.

A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. In order to reassemble any given customer's application (org), someone would need access to our source code in order to reassemble the raw data in a manner that could be interpreted and

understood, and would need the entire set of tapes or disks/arrays supporting a given Instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.

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

For Accenture cloud solution built on AWS and for AWS direct cloud implementations, the following attestations apply.

AWS

AWS System and Organization Controls (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance. There are three AWS SOC Reports:

- AWS SOC 1 Report, available to AWS customers from AWS Artifact
- AWS SOC 2 Security, Availability and Confidentiality Report, available to AWS customers from AWS Artifact
- AWS SOC 3 Security, Availability and Confidentiality Report, publicly available as a whitepaper

Access the AWS SOC Reports at: https://aws.amazon.com/compliance/soc-faqs/.

For additional information about AWS certifications, see the *AWS Certifications, Programs, Reports, and Third-Party Attestations* whitepaper at: https://d0.awsstatic.com/whitepapers/compliance/AWS_Certifications_Programs_Reports_Third-Party_Attestations.pdf.

SALESFORCE

Salesforce has comprehensive privacy and security assessments and certifications performed by multiple third parties. The following audits and their frequencies are performed:

- ISO 27001 - Annually (3-year certification)
- PCI-DSS - Annually
- FedRAMP - Annually
- SOC 1 (SSAE16/ISAE 3402, previously SAS 70) - Twice a year
- SOC 2 & SOC 3 - Twice a year

Copies of our SOC reports can be provided to your Agency upon request and under NDA.

Under NDA, your Agency can also be provided Salesforce's complete FedRAMP Authority to Operate (ATO) package, which contains the following security assessment documentation:

- 01 - Salesforce Government Cloud System Security Plan

- 02 - Salesforce Government Cloud System Security Plan - Tracked Changes
- 03 - Salesforce Government Cloud Attachment 1 - Control Tailoring Workbook (CTW)
- 04 - Salesforce Government Cloud Attachment 2 - Control Implementation Summary (CIS)
- 05 - Salesforce Government Cloud Attachment 3 - PTA and PIA
- 06 - Salesforce Government Cloud Attachment 4 - E-Authentication
- 07 - Salesforce Government Cloud Attachment 5 - FIPS 199 Categorization
- 08 - Salesforce Government Cloud Attachment 6 - User Guide - Customer Configurations
- 09 - Salesforce Government Cloud Attachment 7 - Hardware, Network, and Software System Inventory
- 10 - Salesforce Government Cloud Attachment 8 - Customer Responsibilities
- 11 - Salesforce Government Cloud Rules of Behavior - Ground Rules for Security Success
- 12 - Salesforce Government Cloud Disaster Recovery Plan
- 13 - Salesforce Government Cloud Incident Response Plan
- 14 - Salesforce Government Cloud Configuration Guide
- 15 - Salesforce Government Cloud Continuous Monitoring Plan
- 16 - Salesforce Government Cloud Security Assessment Plan
- 17 - Salesforce Government Cloud Security Assessment Report (SAR)
- 18 - Salesforce Government Cloud Table 4.1 SAR
- 19 - Salesforce Government Cloud Test Cases (SRTM)
- 20 - Salesforce Government Cloud POA&M

IBM CLOUD

IBM follows strict industry guidelines for security, fostering true compliance for the following:

- The ISO 2700 family of standards helps organizations keep information assets secure. IBM is currently certified for ISO 27001, ISO 27017, ISO 27018, ISO 22301, ISO 31000
- SOC 1, SOC 2, SOC 3
- PCI DSS
- HITRUST
- FedRAMP – IBM maintains a FedRAMP Moderate authorization
- HIPAA
- CSA

For additional details please visit: https://www.ibm.com/cloud/compliance

GOOGLE CLOUD

For solutions Accenture implements using Google Cloud, the following attestations apply.

- The ISO 2700 family of standards helps organizations keep information assets secure. Google is currently certified for ISO 27001, ISO 27017, ISO 27018
- SOC 1, SOC 2, SOC 3
- PCI DSS
- HITRUST
- FedRAMP – Google maintains a FedRAMP Moderate authorization to operate for Google Cloud Platform
- HIPAA
- CSA
- NIST 800-53, NIST 800-171

For additional details please visit: https://cloud.google.com/security/compliance/

TWILIO

For solutions Accenture implements using Twilio, the following third-party attestations assure that Twilio has implemented security best practices.

- ISO 27001
- SOC 2
- Privacy Shield
- CSA

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.

Accenture's approach to logging would be tailored to the specific security requirements of a customer. Below are descriptions of specific capabilities that apply to Accenture's cloud solutions built on AWS, AWS implementations, and Salesforce implementations. More information regarding security certifications is included in the response to 8.6.5 above.

AWS

The logging and monitoring of Application Program Interface (API) calls are key components in security and operational recommended practices and requirements for industry and regulatory compliance. AWS customers can leverage multiple AWS features and capabilities, along with third-party tools, to monitor their instances and manage/analyze log files.

AWS CloudTrail

AWS CloudTrail is a web service that records API calls to supported AWS services in an AWS account, delivering a log file to an Amazon Simple Storage Service (Amazon S3) bucket. AWS CloudTrail alleviates common challenges experienced in an on-premise environment by making it easier for customers to enhance security and operational processes while demonstrating compliance with policies or regulatory standards.

With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

- For information on the services and features supported by AWS CloudTrail, visit the AWS CloudTrail FAQs on the AWS website.
- The AWS whitepaper *Security at Scale: Logging In AWS* provides an overview of common compliance requirements related to logging, detailing how AWS CloudTrail features can help satisfy these requirements.
- The AWS whitepaper *Auditing Security Checklist for Use of AWS* provides customers with a checklist to assist in evaluating AWS for the purposes of an internal review or external audit.

AWS CloudTrail: Features and Benefits

Following are some of the many features of AWS CloudTrail:

- **Increased Visibility:** AWS CloudTrail provides increased visibility into user activity by recording AWS API calls. Customers can answer questions such as, “what actions did a given user take over a given time period?” and for a given resource, “which user has taken actions on it over a given time period?”, “What is the source IP address of a given activity?”, and, “Which activities failed due to inadequate permissions?”
- **Durable and Inexpensive Log File Storage:** AWS CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably and inexpensively. Customers can use Amazon S3 lifecycle configuration rules to further reduce storage costs. For example, customers can define rules to automatically delete old log files or archive them to Amazon Glacier for additional savings.
- **Easy Administration:** AWS CloudTrail is a fully managed service; customers simply turn on AWS CloudTrail for their account using the AWS Management Console, the Command Line Interface, or the AWS CloudTrail SDK and start receiving AWS CloudTrail log files in the specified Amazon S3 bucket.
- **Notifications for Log File Delivery:** AWS CloudTrail can be configured to publish a notification for each log file delivered, thus enabling customers to automatically act upon log file delivery. AWS CloudTrail uses the Amazon Simple Notification Service (Amazon SNS) for notifications.
- **Choice of Partner Solutions:** Multiple partners including AlertLogic, Boundary, Loggly, Splunk, and Sumologic offer integrated solutions to analyze AWS CloudTrail log files. These solutions include features like change tracking, troubleshooting, and security analysis. For more information, see the AWS CloudTrail partners section.

- **Log File Aggregation:** AWS CloudTrail can be configured to aggregate log files across multiple accounts and regions so that log files are delivered to a single bucket. For detailed instructions, refer to the Aggregating CloudTrail Log Files to a Single Amazon S3 Bucket section of the user guide.

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications run on AWS. Customers can use Amazon CloudWatch 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, Amazon RDS DB instances, custom metrics generated by customer applications and services, and any log files that 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 and keep their application running smoothly.

Customers can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. Customers can send their existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time. This helps customers better understand and operate their systems and applications, and they can store their logs using highly durable, low-cost storage for later access.

LogAnalyzer for Amazon CloudFront

LogAnalyzer allows customers to analyze their Amazon CloudFront Logs using Amazon Elastic MapReduce (Amazon EMR). Using Amazon EMR and the LogAnalyzer application customers can generate usage reports containing total traffic volume, object popularity, a breakdown of traffic by client IPs, and edge location. Reports are formatted as tab delimited text files, and delivered to the Amazon S3 bucket that customers specify.

Amazon CloudFront's Access Logs provide detailed information about requests made for content delivered through Amazon CloudFront, AWS's content delivery service. The LogAnalyzer for Amazon CloudFront analyzes the service's raw log files to produce a series of reports that answer business questions commonly asked by content owners.

Reports Generated

This LogAnalyzer application produces four sets of reports based on Amazon CloudFront access logs. The Overall Volume Report displays total amount of traffic delivered by CloudFront over the course of whatever period specified. The Object Popularity Report shows how many times each customer object is requested. The Client IP report shows the traffic from each different Client IP that made a request for content. The Edge Location Report shows the total amount of traffic delivered through each edge location. Each report measures traffic in three ways: the total number of requests, the total number of bytes transferred, and the number of requests broken down by HTTP response code. The LogAnalyzer is implemented using Cascading (http://www.cascading.org) and is an example of how to construct an Amazon Elastic MapReduce application. Customers can also customize reports generated by the LogAnalyzer.

SALESFORCE

Logical Access Control

Salesforce internal infrastructure logs are collected by various monitoring tools for activities on the systems that host Salesforce, and include:

- Server access
- Network access
- Firewall management events
- Network intrusion detection systems traffic
- Cache
- Database
- File integrity
- Network device configuration
- Anti-virus detection

Log events are correlated to generate alerts. Alerts are configured to notify the Technical Operations and Computer Security Incident Response Team (CSIRT) teams. Security alerts require acknowledgement and follow up, if appropriate by the CSIRT. Firewalls and IDS systems are configured with automated syslog notifications for key events. Logs are archived and are currently stored for a minimum of (1) one year.

NOTE: These logs are not available to customers.

Customer Auditing Capabilities

Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include:

- **Record Modification Fields:** All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.
- **Login History:** You can review a list of successful and failed login attempts to your organization for the past six months within Salesforce.
- **Field History Tracking:** You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.
- **Setup Audit Trail**: Administrators can also view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to your organization's configuration. This trail can be downloaded into Excel or as a csv file.

While the Login History and Setup Audit Trail are available for six months within Salesforce, audit trails can be downloaded and stored locally to meet longer audit log retention requirements.

Detailed application logs can be used for forensics investigations by customers. These logs are stored for 12 months and are available for a fee.

Event Monitoring (Additional License Option)

In addition to Salesforce's core auditing capabilities, Salesforce also offers Event Monitoring as an additional license option. Your Agency can use event monitoring to discover how often and at what times your users are logging in to and out of your organization. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what reports users are running and exporting and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. Not only can your Agency now better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put your agency at risk. In addition, your agency can also determine if an employee is unnecessarily downloading sensitive customer/citizen information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available.

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

Accenture's solutions provide the capability to restrict visibility of cloud hosted data and documents to specific users or groups. In AWS, this is handled through AWS Identity and Access Management (IAM).

The Salesforce Services infrastructure is divided into a modular architecture based on "Instance". Each Instance is capable of supporting several thousand customers in a secure and efficient manner. Services are grouped within each Instance; with app, search, and database elements contained. There are appropriate controls in place to ensure that any given customer's org (application) is not compromised. The service has been designed to accomplish this and is robustly tested on an ongoing basis by both Salesforce and its customers.

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.

Accenture centrally manages any data breach that results from a security incident through reporting to our Accenture Security Operations Center. In addition, we establish a procedure for managing security incidents for each customer. For cloud work involving AWS, the following capabilities are available to support Accenture's response to a NASPO Purchasing Entity regarding any security incidents.

AWS

AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.

AWS uses a three-phased approach to manage incidents:

1. **Activation and Notification Phase:** Incidents for AWS begin with the detection of an event. This can come from several of the following sources:
   a. Metrics and Alarms: AWS maintains an exceptional situational awareness capability; most issues are rapidly detected from 24/7/365 monitoring and alarming of real-time metrics and service dashboards. The majority of incidents are detected in this manner. AWS uses early indicator alarms to proactively identify issues that may ultimately impact Customers.
   b. Trouble ticket entered by an AWS employee
   c. Calls to the 24/7/365 technical support hotline

If the event meets incident criteria, then the relevant on-call support engineer will start an engagement using AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g. Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.

2. **Recovery Phase:** The relevant resolvers will perform break fix to address the incident. Once troubleshooting, break fix, and affected components are addressed, the call leader will assign next steps in terms of follow-up documentation, follow-up actions, and end the call engagement.
3. **Reconstitution Phase:** Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions such as design changes, etc. will be captured in a Correction of Errors (COE) document and tracked to completion.

In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

AWS’s incident management program is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001, and FedRAMP compliance.

Workflow documentation of Content (data) is the responsibility of AWS Customers as Customers retain ownership and control of their own guest operating systems, software, applications, and data.

SALESFORCE

As determined for a specific statement of work, Salesforce can promptly notify the Customer in the event Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce support, email to customer's administrator and Security Contact (if submitted by customer), and public posting on trust.salesforce.com.

Salesforce maintains an Incident Response Plan and has an established Security Incident Response Process. During a security incident, the process guides Salesforce personnel in management,

communication, and resolution activities. Government customers can report security incidents related to their Salesforce products and offerings via security_gov@salesforce.com. Salesforce will respond in accordance with the incident response process described above.

The Salesforce incident response plan/process was created in accordance with FedRAMP moderate control requirements which include incident response requirements derived from NIST SP 800-53, NIST SP 800-61, and the FedRAMP Incident Communications Procedure.

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.

The following describes the capabilities within AWS that Accenture leverages for AWS solutions, including our cloud offerings built on AWS, to meet specific customer requirements related to zones of control. Accenture anticipates that most customers will want to leverage the multi-tenant model within AWS to maximize the cost effectiveness of cloud solutions.

AWS

Single and Multi-Tenant Environments

The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate customers from each other. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.2 published in April 2016.

More information on AWS's multi-tenant architecture is found in the *AWS Risk and Compliance* whitepaper.

AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS Cloud while isolating your Amazon EC2 compute instances at the hardware level. AWS isolation and deployment options are illustrated in Figure 9.

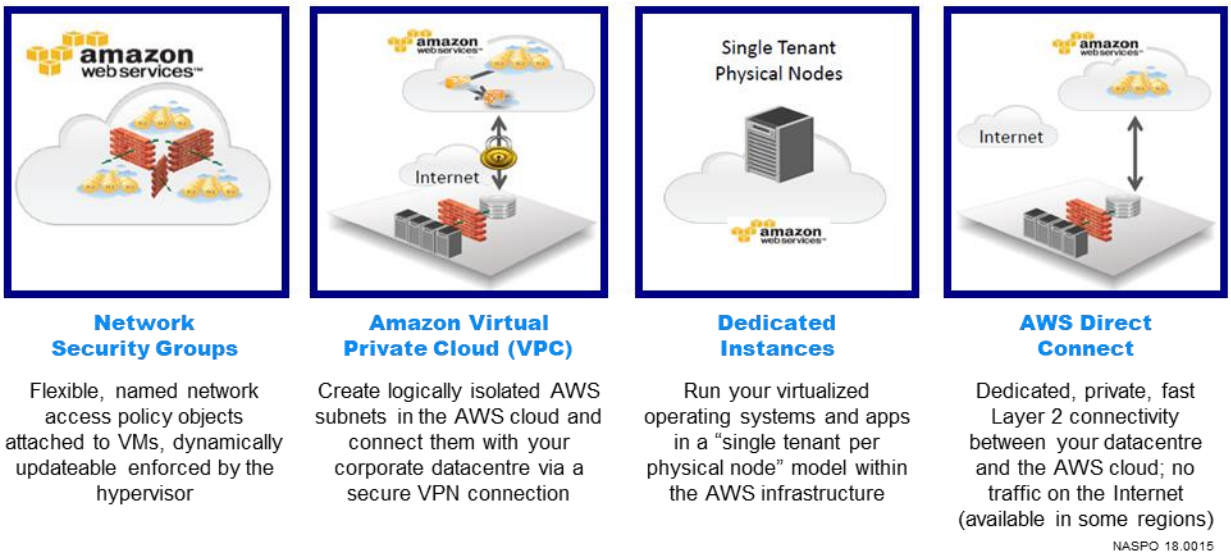


Figure 9. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS Cloud while isolating your Amazon EC2 compute instances at the hardware level.

SALESFORCE

A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. In order to reassemble any given customer's application (org), someone would need access to our source code in order to reassemble the raw data in a manner that could be interpreted and understood, and would need the entire set of tapes or disks/arrays supporting a given Instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.

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).

Accenture understands that security in the public cloud has long been a concern of both enterprises and government entities when considering a move to cloud IaaS and PaaS. Accenture has developed a Security Reference Architecture for cloud environments covering public and private cloud for IaaS, public cloud for PaaS and SaaS. This general Security Reference Architecture has been customized for each of the public cloud providers to specify what tools from the provider to use for each of the layers of security.

Generally, Accenture's Security Reference Architecture describes the security services that come native from the cloud provider, services that must be configured by the customer, and services that Accenture provides to complete the security architecture. We describe the following category of services:

- Governance and Risk Management
- Foundation Security (includes connectivity)

- Digital Identity
- Data Privacy and Protection
- Application Security
- Cyber Defense

AWS

In an AWS environment for Foundation Security, AWS provides Virtual Private Cloud, Security Groups, Network Access Control Lists, Regions, Availability Zones, and the ability to manage Accounts and Organizations. As the cloud service provider, Accenture would work with the customer to configure these security tools for the customer's needs. Additionally, through the Accenture Cloud Platform, Accenture would provide capabilities at the Foundation Security layer for System/OS Hardening, Intrusion Detection/Prevention, Malware treatment, System Integrity, and Server/Endpoint Security. This is an example of one layer if our security Reference Architecture was implemented with one public cloud provider – AWS. Because Accenture has spent significant resources developing this Security Reference Architecture, we are not including all the details in this document, but would share those details with specific Purchasing Entities when engaging them for cloud services under this proposed arrangement.

SALESFORCE

Salesforce offers market leading PaaS and market leading SaaS solutions. Salesforce does not provide IaaS as a direct service offering to our customers, it is an underlying part of our PaaS and SaaS offerings.

The Salesforce Platform is built for cloud computing, with multitenancy inherent in its design. To meet the high demands of its large user population, Force.com's foundation is a metadata-driven software architecture that enables multi-tenant applications.

Force.com combines several different persistence technologies, including a custom-designed relational database schema, which are innately designed for clouds and multitenancy—no virtualization required.

Force.com's core technology uses a runtime engine that materializes all application data from metadata—data about the data itself. In Force.com's well-defined metadata-driven architecture, there is a clear separation of the compiled runtime database engine (kernel), tenant data, and the metadata that describes each application. These distinct boundaries make it possible to independently update the system kernel and tenant-specific applications and schemas, with virtually no risk of one affecting the others.

Every logical database object that Force.com exposes is internally managed using metadata. Objects, (tables in traditional relational database parlance), fields, stored procedures, and database triggers are all abstract constructs that exist merely as metadata in Force.com's Universal Data Dictionary (UDD). For example, when you define a new application object or write some procedural code, Force.com does not create an actual table in a database or compile any code. Instead, Force.com simply stores metadata that the system's engine can use to generate the virtual application components at runtime. When you need to modify or customize something about the application schema, like modify an existing field in an object, all that's required is a simple non-blocking update to the corresponding metadata.

Because metadata is a key ingredient of Force.com applications, the system's runtime engine must optimize access to metadata; otherwise, frequent metadata access would prevent the service from scaling. With this potential bottleneck in mind, Force.com uses massive and sophisticated metadata caches to maintain the most recently used metadata in memory, avoid performance-sapping disk I/O and code recompilations, and improve application response times.

The multitenant architecture and secure logical controls address separation of Customer Data. The Salesforce infrastructure is divided into a modular architecture based on "instances". Each instance is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the instance architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer's Salesforce instance from being compromised. This functionality has been designed and undergoes robust testing through an on-going process by both Salesforce and its customers.

These papers further explain the technology that makes the Salesforce Force.com platform fast, scalable, and secure for any type of application:

- https://developer.salesforce.com/page/Multi_Tenant_Architecture
- https://developer.salesforce.com/page/Secure_Private_Trustworthy_Force.com_Whitepaper
- https://developer.salesforce.com/page/An_Overview_of_Force.com_Security

8.6.11 - Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Accenture works to minimize access to our customer's sensitive data, but has procedures in place to perform background checks for all our employees and subcontractors who would have access to sensitive data. In addition, Accenture implements several Client Data Protection controls to manage access to sensitive data including regular reviews of an individual's access, least privilege access, regular training on how to handle sensitive data, proper data disposal, and reviews of SIEM logs.

8.6.12 - Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

For Accenture solutions on AWS, the following measures apply for security data at rest and in transit. Accenture's cloud offerings built on AWS leverage the AWS encryption capabilities to secure data at rest and in transit.

AWS

Data at Rest

There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions (such as AWS Key Management Service [KMS]) to manual, client-side options (such as AWS CloudHSM). Choosing the right solutions depends on which AWS Cloud services are being used and customer requirements for key management. Information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon Simple Storage Service (Amazon S3) Developer Guide.

Additionally, the *Encrypting Data at Rest* whitepaper provides an overview of the options for encrypting data at rest in AWS Cloud services. It describes these options in terms of where encryption keys are stored and how access to those keys is controlled. Both server-side and client-side encryption methods are discussed with examples of how each can be accomplished in various AWS Cloud services.

Data in Transit

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers and network traffic between servers.

Services from AWS provide support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

The *AWS Security Best Practices* whitepaper provides greater detail on how to protect data in transit and at rest in the AWS Cloud.

SALESFORCE

Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements.

Data at Rest

Salesforce includes a feature to encrypt custom text fields (ECF). The fields can be masked appropriately for specific data types (i.e., credit card number, Social Security Number, National Insurance Number, Social Insurance Number).

Access to read the masked parts of the fields is limited by the "View Encrypted Data" permission, which is not enabled by default.

Customers can manage their encryption key based on their organization’s security needs and regulatory requirements. See our Help and Training site for details:
https://help.salesforce.com/apex/HTViewHelpDoc?id=security_keys_using_master.htm&language=en

Encrypted fields are encrypted with 128-bit keys and use the AES (Advanced Encryption Standard) algorithm.

Additional Salesforce Encryption Capabilities

Apex Code extends the powerful and proven success of the Force.com platform by introducing the ability to write code that runs on Salesforce servers. This language makes possible the development of a new class of application and features deployed entirely on demand. Using Apex, your Agency can create user interface classes that utilize the Apex crypto class to encrypt field level data up to AES 256-bit encryption. For more information:
https://www.salesforce.com/us/developer/docs/apexcode/Content/apex_classes_restful_crypto.htm

Third Party Encryption Solutions (Additional License Option)

Should additional encryption be required, third-party solutions such as CipherCloud, Skyhigh, and PerspecSys are available on the Salesforce AppExchange. These solutions offer data loss prevention, user activity and monitoring, malware protection, as well as data protection with encryption and tokenization. Data can be encrypted and masked at rest, keys managed and stored in Salesforce, and compliance controls to prevent unauthorized access to data and keys.

Data in Transit

All transmissions between the user and the Salesforce Services are TLS encrypted with a 2048-bit Public Key. The Services use International/Global Step Up TLS certificates, with AES 256-bit encryption by default.

8.6.13 - Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Accenture centrally manages any data breach that results from a security incident through reporting to our Accenture Security Operations Center (ASOC). In addition, we establish a procedure for managing security incidents for each customer, which would include the procedures for notifying the participating entity and any customers of a data breach. In the event of a data breach, Accenture would work with our ASOC to bring in any necessary resources to quickly resolve the underlying issue and restore services to normal operations.

8.7 (E) MIGRATION AND REDEPLOYMENT PLAN

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.

The end of life activities for each Purchasing Entity would vary based on the type of service being deprovisioned. Accenture would notify the Purchasing Entity, for which we are providing services, in advance of any end of life service and work to develop a plan to export and transition data. Each of our services provides multiple methods of exporting data for redeployment, which means that a customer's data is very portable to a new solution. Data security can be maintained by using the cloud provider's encryption mechanism or by exporting data and encrypting it with a 3rd party tool. Redundancy is supported through the inherent redundancy of the cloud solution and data redundancy is maintained until the service is terminated.

SALESFORCE

Salesforce claims no ownership rights to customer data and customer data is only utilized as the customer instructs or to fulfill contractual or legal obligations. Salesforce is responsible for maintaining access in terms of performance and availability to the data. Salesforce provides contractual assurance to its customers that the data hosted in Salesforce's services will be kept confidential and not accessed by third parties except under narrow circumstances (such as support issue). In such circumstances, we will access your org only with prior approval and subject to the Non-Disclosure Agreement (NDA).

Participating entities have full rights to extract the data via Export Services utilities including: weekly export, data loader, APIs, EAI tools, etc. Below we describe the methods to export data from Salesforce:

- Direct Export - Data can be exported directly into CSV (comma separated values) file, or Excel files with a button click. This can be done from either a standard or custom list view, or from a report. This is the most common method utilized by end users.
- Excel Connector - Salesforce provide an Excel Connector to push and pull data from Excel to Salesforce.com and vice versa.
- Salesforce API - Data can be exported to and from the system through our API at any time or via a number of built in features.
- Salesforce Data Loader - The Salesforce Apex Data Loader is a free tool which is used specifically for importing/updating/exporting data in Salesforce.
- Partner Tools - There are also many pre-integrated partner tools, some of which you may already own that may be leveraged. Examples of these include, but are not limited to, Informatica, Pervasive, CastIron, Boomi, etc.

We also offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system).

Data and artifacts can be exported with CRON-like scheduling, or on demand. In the event of an export, all data visibility and record access rules are enforced, and the requestor only obtains the data allowed under the participating entity's security policy.

In the event of termination of the Salesforce service, requests made within 30 days after the effective date of termination or expiration of the Subscription Agreement, Salesforce will make your data available to you for export or download. Once the export has been completed, an email will be sent to you containing a link where you can download a .zip file that contains multiple .csv (spreadsheets) files, each representing your Salesforce objects. Your data on disk is flagged within the database and set to inactive status or what can be referred to as a "soft delete." This data is no longer available or accessible to the application but is backed up in the full database backup process. The data remains in this state for 180 days; this is done in the event that the customer decides to resume services or needs the data for a legal reason. At 180 days, the data is marked for deletion ("hard delete") and will be deleted after 30 more days. Once this "hard delete" is executed the customer data is physically deleted and non-recoverable from the database. Following the purge, the data will remain on backup for an additional 90 days prior to being overwritten and unrecoverable.

Salesforce also provides tools that support the migration of configurations and customizations to the different environments, such as local code repositories, sandboxes and production. These tools can be

used to export your configurations and customizations in the event you terminate your relationship with Salesforce.

The available tools are as follows:

- Metadata API: Salesforce provides a metadata API that allows for programmatic access to the metadata in a customer's Salesforce environment.
- Force.com IDE: The Salesforce Force.com IDE is an integrated development environment that is built on top of the Eclipse open source IDE.
- Force.com Migration Tool: A Java/Ant-based command-line utility for moving metadata between a local directory and a Salesforce organization. Migrating from stage to production is done by IT. Anyone that prefers deploying in a scripting environment will find the Force.com Migration Tool a familiar process.

For additional details on Salesforce environment management, please see the following:

- https://developer.salesforce.com/page/Force.com_Migration_Tool
- http://www.salesforce.com/us/developer/docs/api_meta/index.htm
- http://wiki.developerforce.com/index.php/Force.com_IDE

Migration to a New Solution or Cloud Service Provider

In the event a migration is required, Salesforce recommends the migration be led by a qualified implementation partner, such as Accenture, to assist with the migration.

Depending on the type of migration (e.g., "Like for Like" replace vs. business transformation) the level of effort can vary significantly. Large system integrators will have data migration practices that specialize in this type of work who are familiar with anticipated challenges and related solutions.

As outlined above, Salesforce makes it extremely easy for your Agency to export its data whenever needed, so most of the expense of migrating off of Salesforce will be the cost of implementing and loading data into the new target solution.

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.

The Purchasing Entity would have access to and maintain ownership of their data. Therefore, they would be able to download or access the data through a variety of means depending on the service being provided. From an SLA perspective, data is maintained in our cloud solutions at least until the cloud service is fully terminated, but in many cases, the data is not permanently deleted until a later grace period has expired.

8.8 (E) SERVICE OR DATA RECOVERY

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)."

Accenture is proposing services that are redundant by nature. This is one of the benefits of using cloud services and would be a design characteristic that Accenture would build into cloud solutions that we offer to purchasing entities under this contract. However, Accenture recognizes that even cloud architectures are not perfect and we have to plan for the ability to recover from unexpected or catastrophic events. If one of these situations occurs, Accenture would communicate regularly with the customer to describe the event and the current status. For Accenture cloud solutions implemented on AWS, Accenture uses replication across multiple physical locations (Availability Zones in AWS terms) as a minimum mitigation against DR scenarios. We can also implement replication across multiple regions to further reduce the possibility of any data being lost. Each of our solutions has the ability to support an RTO of 4 hours.

AWS

Many public-sector organizations are realizing the benefits of using AWS to enable faster Disaster Recovery (DR) of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS Cloud supports many popular DR architectures from “pilot light” environments that are ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover. With data centers in 18 regions around the world (five in the US), AWS provides a set of cloud-based DR services that enable rapid recovery of IT infrastructure and data.

General DR/COOP and Backup Requirements and Issues

Following are some of the minimum needs and requirements in a traditional DR approach:

- Facilities to house additional infrastructure, including power and cooling.
- Security to confirm the physical protection of assets.
- Suitable capacity to scale the environment.
- Support for repairing, replacing, and refreshing the infrastructure.
- Contractual agreements with an Internet Service Provider (ISP) to provide Internet connectivity that can sustain bandwidth utilization for the environment under a full load.
- Network infrastructure such as firewalls, routers, switches, and load balancers.
- Enough server capacity to run all mission-critical services, including storage appliances for the supporting data, and servers to run applications and backend services such as user authentication, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), monitoring, and alerting.

SALESFORCE

Extended Downtime

Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers’ trust. To ensure

maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.

Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status.

The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds, all with an average up time of 99.9+ percent.

Unrecoverable Loss

To maximize availability, the service is delivered using multiple world-class data centers supporting primary and replicated disaster recovery instance, plus a separate production-class lab. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high-availability servers and network technologies, and a carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with maximum uptime and performance.

The Salesforce services are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, Salesforce has more than one piece of redundant equipment for a given function.

Experiences a Business Failure

Salesforce has documented Disaster Recovery and Business Continuity plans for critical business functions. The Disaster Recovery and Business Continuity plans are tested at least annually. A post mortem documenting the results of the disaster recovery tests can be provided to customers with a signed NDA in place.

Business continuity plans are updated each year, including the list of business processes, recovery time objectives, and key resources. Senior management is included in this process. Business continuity plans are exercised on an annual basis. Action items and lessons learned are tracked from each incident and exercise conducted. Action items are prioritized and tracked until closed. Salesforce has developed additional procedures, processes and plans, including a Pandemic plan.

Salesforce also recommends customers also devise their own backup strategy for their data, as there is a fee for customers to request for restoration from Salesforce backups. Salesforce provides multiple ways for our customers to obtain periodic backups of its data. We offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system). Salesforce also supports data replication, which allows customers to store and maintain a local, separate copy of their organization's Salesforce data including the META data (logins,

etc.) for specialized uses, such as data warehousing, data mining, custom reporting, analytics, and integration with other applications. Data replication provides customers with local control and the ability to run large or ad hoc analytical queries across the entire data set. Backup and Recovery Best Practices and additional information can be found in this Help & Training article: https://help.salesforce.com/HTViewSolution?id=000213366&language=en_US

Ability to recover within 4 hours

Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, and backed up at the primary data center. Backups are performed daily at the primary data center facility without stopping access to the application.

RPO and RTO

For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4-hour recovery point objective (RPO) and 12-hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and the participating entity.

> 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."

Accenture cloud solutions build on AWS include daily backups of critical data into separate locations within the continental United States. Below is more information about AWS and Salesforce capabilities.

AWS

AWS Capabilities for DR/COOP/Backup Solutions

With AWS, customers can eliminate the need for additional physical infrastructure, off-site data replication, and upkeep of spare capacity. AWS uses distinct and geographically diverse Availability Zones that are engineered to be isolated from failures in other Availability Zones. This innovative and unique AWS feature enables customers to protect applications from the failure of a single location, resulting in significant cost savings and increased agility to change and optimize resources during a DR scenario.

AWS offers the following high-level DR capabilities:

- **Fast Performance:** Fast, disk-based storage and retrieval of files.
- **No Tape**: Eliminate costs associated with transporting, storing, and retrieving tape media and associated tape backup software.
- **Compliance:** Minimize downtime to avoid breaching Service Level Agreements (SLAs).
- **Elasticity:** Add any amount of data, quickly. Easily expire and delete without handling media.

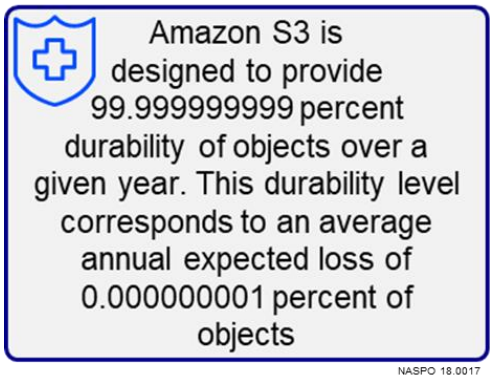
- **Security:** Secure and durable cloud DR environment with industry-recognized certifications and audits.
- **Partners:** AWS solution providers and system integration partners to help with deployments.

Solution Use Cases

AWS can enable customers to cost-effectively operate multiple DR strategies. Figure 10 shows a spectrum of scenarios: “backup and restore,” “pilot light,” “warm standby,” and “multi-site,” arranged by how quickly a system can be available to users after a DR event.

Figure 10. AWS can enable customers to cost-effectively operate multiple DR strategies.

Following is a detailed description of each DR option:



- **Backup and Restore**: In most traditional environments, data is backed up to tape and sent off-site regularly. Recovery time will be the longest using this method, and lack of automation leads to increased costs. Using Amazon Simple Storage Service (Amazon S3) is ideal for backup data, as it is designed to provide 99.999999999 percent durability of objects over a given year. Transferring data to and from Amazon S3 is typically done via the network, and it is therefore accessible from any location. Also, with AWS Storage Gateway, customers can automatically back up on-premises data to Amazon S3.
- **Pilot Light for Simple Recovery into AWS Warm Standby Solution**: The idea of the pilot light is an analogy that comes from the gas heater. In a gas heater, a small idle flame that is always on can quickly ignite the entire furnace to heat up a house as needed. This scenario is analogous to a backup and restore scenario; however, customers must verify that they have the most critical core elements of their system already configured and running in AWS (the pilot light). When the time comes for recovery, customers would rapidly provision a full-scale production environment around the critical core.
- **Warm Standby Solution in AWS**: The term “warm standby” is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. It further decreases recovery time because, in this case, some services are always running. By identifying business-critical systems, customers could fully duplicate these systems on AWS and have them always on.
- **Multi-site Solution Deployed on AWS and On-site**: A multi-site solution runs in AWS and on a customer’s existing on-premises infrastructure in an active-active configuration. During a disaster

situation, an organization can simply send all traffic to AWS servers, which can scale to handle their full production load.

DR Resources

There are multiple resources to help organizations start using AWS for a DR/COOP and backup solution:

- Read the AWS whitepaper *Using AWS for Disaster Recovery*
- Read the Forrester whitepaper *File Storage Costs Less in the Cloud than In-House*
- Read the Enterprise Strategy Group whitepaper *Amazon Web Services: Enabling Cost-Efficient Disaster Recovery Leveraging Cloud Infrastructure*
- Review a sample AWS DR architecture
- Review more information on AWS DR capabilities and approaches

SALESFORCE

Methods of Data Backups

Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the primary data center, and then cloned to the disaster recovery data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.

Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.

The backup retention policy is 90 days (30 days for sandboxes). Deleted/modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.

Methods of server image backups

Each server has been allocated a different volume group so it can fail over to its backup server within the instance independently of the others.

Digital location of backup storage

Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.

Alternate data center strategies

Customer Data for customers in Salesforce's Government Cloud is stored in two of our U.S. data center locations.

The Salesforce service performs near real-time replication at each data center and annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center. The disaster recovery site is a 100% replica of the primary production site of capacity (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location.

8.9 (E) DATA PROTECTION

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.

Participating entities retain control and ownership of their data. There are multiple options for storing data in the cloud solutions that we offer. For sensitive data, we would work with the customer to develop their solution.

All data stored by the cloud solutions on behalf of customers gives strong tenant isolation security and control capabilities. Customers should consider the sensitivity of their data and decide if and how they will encrypt data while it is in transit and while it is at rest.

Please refer to the response to 8.6.12 for more details. Note that the answers apply to all three service models. For IaaS and some PaaS solutions, the customer has input on how the encryption is configured. Accenture would work with the customer to configure appropriate encryption in transit and at rest.

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.

Accenture asserts that it is willing to sign relevant and applicable Business Associate Agreements or any other agreements that may be necessary to protect data with a Purchasing Entity.

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.

Accenture would only use data for the purposes defined in the contract, a specific statement of work, or related service level agreement. We would not use government data or government related data for any purpose outside the confines of the contract including, but not limited to data mining. Accenture would not resell or otherwise redistribute information gained from its access to the data received as a result of this RFP, nor would we allow our subcontractors to do the same.

Any proposed use of government data not explicitly defined in a specific statement of work would be formally requested from the entity we are working with.

8.10 (E) SERVICE LEVEL AGREEMENTS

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.

Traditionally, organizations establish SLAs and Operational Level Agreements (OLAs) through a series of negotiations between end users or portfolio owners and the operations team. Many organizations revisit expectations for their SLAs and OLAs due to the degree of change in capability. When following best practices for cloud adoption, customers often find that SLAs and OLAs for traditional things like uptime or availability for individual components will become irrelevant over time. Therefore, instead of reusing existing SLAs and OLAs for their cloud workloads, we encourage our customers to shift from an IT-centric view to a user-centric view of IT service delivery. With this approach in mind, Accenture's cloud solutions include the ability to negotiate a Service Level Agreement that supports our customer's business operations.

AWS

Following recommended practice guidance, implementing automation, and reusing effective cloud architecture patterns gives development teams the ability to readily implement highly available solutions. With AWS's automated failure detection and recovery, systems can fail and recover without affecting users of the IT environment. AWS customers can build highly resilient systems in the cloud by employing multiple instances in multiple Availability Zones and data replication to achieve extremely high Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and service availability.

SALESFORCE

Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately.

The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds all with an average up time of 99.9+ percent.

Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status.

Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are a leader in availability. To ensure maximum

uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.

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.

Accenture's Service Levels are inherently dependent on the underlying cloud services provider. For solutions built on AWS, the approach to service levels applies below. See response to 8.10.1 for more details on approach to Service Level Agreements.

AWS provides Service Level Agreements (SLAs) that apply to customer use of specific services. Due to the rapidly evolving nature of AWS Cloud service offerings, their SLAs are best reviewed directly on the AWS website via the links below:

- Amazon Compute SLA: http://aws.amazon.com/ec2-sla/
- Amazon Simple Storage Service (Amazon S3) SLA: http://aws.amazon.com/s3-sla
- Amazon CloudFront SLA: http://aws.amazon.com/cloudfront/sla/
- Amazon Route 53 SLA: http://aws.amazon.com/route53/sla/
- Amazon Relational Database Service (Amazon RDS) SLA: http://aws.amazon.com/rds-sla/
- AWS Shield Advanced SLA: https://aws.amazon.com/shield/sla/

8.11 (E) DATA DISPOSAL

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

Accenture's cloud solutions built on AWS leverage AWS disposal procedures. Below is specific information on AWS and Salesforce Data Disposal.

AWS

There are no long-term contracts with AWS and customers can terminate their relationship with AWS at any time. Click on the below links to view the full language of the AWS Customer Agreement and Service Terms:

- AWS Customer Agreement: http://aws.amazon.com/agreement/
- AWS Service Terms: http://aws.amazon.com/service-terms/

Before closing your account, back up any applications and data that you want to retain. AWS will not be able to retrieve your account data after your account is closed. Hardware used by a closed account is eventually allocated to other accounts, but no other accounts will ever have access to the data you stored on that hardware. If you are concerned about the data on your AWS resources, you can manually terminate or delete resources before closing the account.

AWS classifies all media entering AWS facilities as critical and treats it accordingly, as high impact, throughout its lifecycle. To destroy data on storage devices, as part of the decommissioning process in accordance with the AWS security standard, following are the equipment use procedures:

- Every AWS data center facility contains one approved degaussing device and one approved disk destruction device.
- Equipment containing storage media is checked to confirm that any data or software has been removed or securely overwritten prior to disposal or reuse.
- The functionality of all media sanitization equipment is checked for operational readiness at regular intervals.
- All solid-state drives (SSDs) are wiped prior to crushing.
- All hard drives and magnetic tapes are degaussed after being removed from a device and placed in a secure bin.
- Degaussing and destruction device functionality is tested on a periodic basis to verify that the intended sanitization is being achieved.

Portable storage devices (e.g. external hard drives, floppy disks, storage tapes, compact discs, digital video discs, USB flash/thumb drives, and diskettes except for those that are part of an approved device, such as a flash card that is part of a networking router) are not permitted for use within the system boundary.

SALESFORCE

Data Disposal and Destruction

In the event of termination of the Salesforce service, requests by a participating entity made within 30 days after the effective date of termination or expiration of the Subscription Agreement, Salesforce will make your data available to you for export or download. Once the export has been completed, an email will be sent to you containing a link where you can download a .zip file that contains multiple .csv (spreadsheets) files, each representing your Salesforce objects. Your data on disk is flagged within the database and set to inactive status or what can be referred to as a "soft delete." This data is no longer available or accessible to the application but is backed up in the full database backup process. The data remains in this state for 180 days; this is done in the event that the customer decides to resume services or needs the data for a legal reason. At 180 days, the data is marked for deletion ("hard delete") and will be deleted after 30 more days. Once this "hard delete" is executed the customer data is physically deleted and non-recoverable from the database. Following the purge, the data will remain on backup for an additional 90 days prior to being overwritten and unrecoverable.

Media Sanitization

Salesforce has an established process for sanitizing media consistent with industry guidelines and consistent with NIST SP 800-88 Guidelines for Media Sanitization [MP-6].

8.12 (E) PERFORMANCE MEASURES AND REPORTING

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.

Accenture's solutions are built upon services provided by our partners or subcontractors such as AWS and Salesforce. Therefore, our ability to guarantee reliability and uptime greater than 99.9 percent is dependent on the specific services and reliability of our partners or subcontractors. In the case of AWS, the planned IaaS and PaaS services provide uptime of at least 99.9 percent so Accenture would be able to offer that availability to participating entities. Accenture will work with participating agencies to engage the cloud hosting provider on the specific SLAs we could commit to for a specific set of services. Each specific statement of work would have consequences or SLA remedies based on the business need.

Below is the overall AWS approach for Performance Measures and Reporting.

AWS

AWS takes extensive precautions to help verify that they will remain fully operational, with no loss of service for AWS hosted applications. AWS replicates critical system components across multiple Availability Zones to confirm high availability both under normal circumstances and during disasters such as fires, tornadoes, or floods. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and are housed in separate facilities. Each AWS Availability Zone runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single Availability Zone. The data centers' electrical power systems are designed to be fully redundant and maintainable without impact to operations. Common points of failure, such as generators, UPS units, and air conditioning are not shared across Availability Zones.

At AWS, they plan for failure by maintaining contingency plans and regularly rehearsing responses. AWS regularly performs preventative maintenance on their generators and UPS units to confirm that equipment is ready when needed. AWS also maintains a series of incident response plans covering both common and uncommon events, and update them regularly to incorporate recommended practices and prepare for emerging threats. In the days leading up to a known event such as a hurricane, AWS would prepare by increasing fuel supplies, updating staffing plans, adding provisions like food and water to verify the safety of the support teams, etc. Once it is clear that a storm will impact a specific region, the response plan is executed and they post updates to the Service Health Dashboard throughout the event.

Note that AWS far exceeds the Uptime Institute Tiering certification. Tiering aspects do not take into consideration the nature of the services of the cloud environment, and although the uptime institution tiering can be a great guide, it ultimately does not accurately map to a cloud service provider organization. AWS does not have a Certified Uptime Tiering level; however, they operate a data center environment using N+1 architecture. AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.95 percent, and Amazon S3 with an SLA of 99.9 percent. AWS generator backup capabilities are detailed in their System and Organization Control (SOC) Reports (as is a discussion regarding business continuity planning and N+1 architecture).

While AWS goes to great lengths to provide availability of the cloud, their customers share responsibility for confirming availability within the cloud. These customers and others like them have succeeded because they designed for failure and have adopted recommended practices for high availability, such as taking advantage of multiple Availability Zones and configuring Auto Scaling groups to replace unhealthy instances. The *Building Fault-Tolerant Applications on AWS* whitepaper is a great introduction to achieving high availability in the cloud. In addition, the AWS Well-Architected Framework codifies the experiences of thousands of customers, helping customers assess and improve their cloud-based architectures and mitigate disruptions.

In addition, the AWS Architecture Center is designed to provide customers with the necessary guidance and application architecture recommended practices to build highly scalable and reliable applications in the AWS Cloud. These resources will help you understand the AWS Cloud, its services and features, and will provide architectural guidance for design and implementation of systems that run on the AWS infrastructure.

AWS customers can rest assured that services and Availability Zones help provide the most solid foundation upon which to build a reliable application.

Please refer to the sample fault-tolerant architecture in Figure 11.

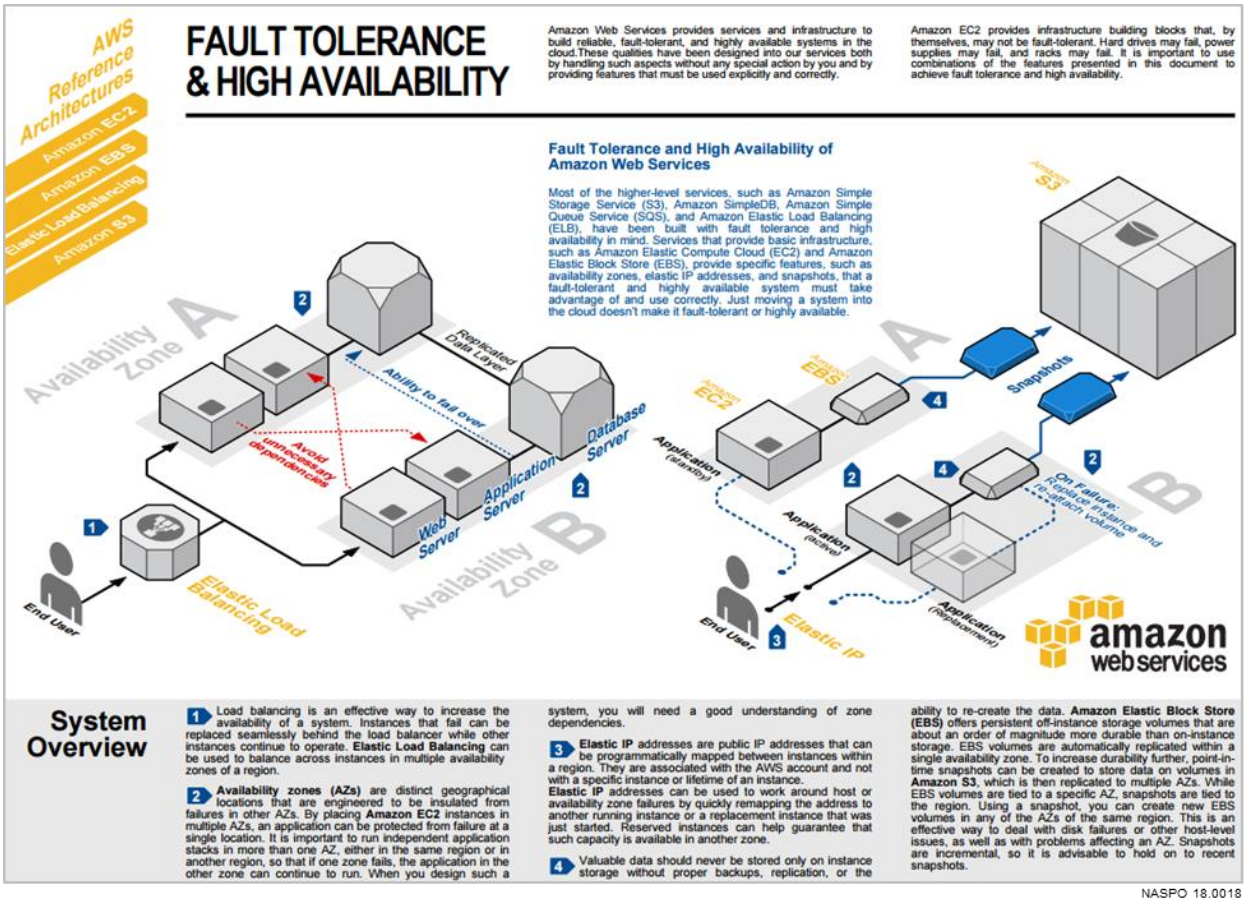


Figure 11. As shown in the fault tolerant sample of AWS architecture, AWS customers can rest assured that services and Availability Zones help provide the most solid foundation upon which to build a reliable application.

SALESFORCE

Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are a leader in availability. To ensure maximum uptime and continuous availability, Salesforce provides redundant data protection and advanced facilities protection, along with a complete data recovery plan—all without affecting performance.

Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status.

The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per

day with an average request response time of less than .25 seconds all with an average up time of 99.9+ percent.

Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately.

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

Accenture's procedures and schedules for downtimes are determined based on client need. For many services, such as the Accenture Cloud Platform, we define a default schedule, but that can be customized for our customer. Please see response to 8.12.1 above for more information on AWS SLA criteria.

SALESFORCE

Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately.

Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status.

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.

For Accenture solutions built on AWS and for AWS cloud services, Accenture would have an assigned Client Service Deliver Manager (CSDM) that the participating entity would contact for support. The CSDM would leverage the Accenture assigned to the project to provide the support for the participating entity. Below is more information on how Salesforce support is handled.

SALESFORCE

Salesforce is proposing the Premier+Success Plan. Participating entities can cover all of its bases with this plan: support, training, and administration. It's what the + is all about. The Premier+ Success Plan gives you all the benefits of our Premier success plan, including a support rep assigned to your organization, priority case routing, one-hour response time, 24x7 phone support, unlimited usage of our entire online course library, plus one very helpful addition: access to your own team of expert Salesforce administrators. This lets you focus on design and management while we support your configuration.

The Premier+ Success Plan includes:

- Unlimited access to our entire online course catalog of 100+ courses
- 24x7 toll-free phone support
- Priority case queuing and routing

- Quick one-hour response time
- An assigned support account rep
- Force.com code troubleshooting
- Customizable end-user course templates
- Premier Success Review to measure usage and trends
- Access to our pool of Salesforce Certified Administrators who can configure and maintain your Salesforce edition
- Premier Success Review to measure usage and trends
- Includes administration services: Get configuration help. Request 100+ routine configuration updates like creating users, reports, workflow, and dashboards. You take online administration training to learn the basics, then you tell us your business requirements. Our team of certified administrators updates your Salesforce system.

Please see the Premier+ Success Plan terms for more information:
http://www2.sfdcstatic.com/assets/pdf/misc/salesforce_premierplans.pdf

Subject to the Government Cloud Premier+ Success Plan outlined above, access to systems and permissions which could permit access to Customer Data inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and FFRDC Customer Data will be restricted to Qualified U.S. Citizens. Qualified US Citizens are individuals who are United States citizens, and are physically located within the United States when accessing the Salesforce Government Cloud systems; and have completed a background check as a condition of their employment with Salesforce.

Severity Levels & Response Times

Issues will be categorized and handled according to an assigned severity level, as follows:

Level 1 - Critical
Response time: One Hour*

Critical production issue affecting all users, including system unavailability and data integrity issues with no workaround available.

Level 2 - Urgent
Response time: Two Hours*

Major functionality is impacted or significant performance degradation is experienced. Issue is persistent and affects many users and/or major functionality. No reasonable workaround available. Also includes time-sensitive requests such as requests for feature activation or a data export.

Level 3 - High
Response time: Four Hours**

System performance issue or bug affecting some but not all users. Short-term workaround is available, but not scalable.

Level 4 - Medium
Response time: Eight Hours**

Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Reasonable workaround available. Resolution required as soon as reasonably practicable.

*24/7 Severity 1 and 2 coverage includes weekends and holidays

**Severity 3 and 4 target response times include local business hours only and exclude weekends and holidays.

Overview of Support Escalation Path

An issue is received by Tier 1 Support Rep who will document details and attempt to resolve. In the event that the problem cannot be resolved at this level, case will be escalated to a Tier 2 Support Rep for further analysis. Occasionally, a Case may be received for which technical understanding or indicated fix exceeds the responsibility of Support. These issues are quickly brought to the attention of R&D through the Tier 3/QA channel. Throughout the lifecycle of the case, customer will receive regular updates from the case owner at regular intervals based on case severity. Customers can work with their Support Account Specialist (SAS) if assigned through the purchase of Premier Support as a point of escalation should the need arise.

Step-by-step escalation path:

- Case is logged via Help Portal, Phone or through Live Chat.
- Depending on the functional area of the case a Tier 1 Support Rep from the appropriate skill group responds to the user confirming that the issue has been received and is in process.
- Tier 1 analyzes the issue from the perspective of customer provided information in the case.
- Tier 1 makes contact (phone or email) with the customer and gathers more information including any access needed to reproduce the problem.
- With all necessary information gathered, Tier 1 will attempt to resolve the issue with the customer.
- When resolution cannot be immediately achieved, Tier 1 Support Rep will escalate to a Tier 2 Support Rep in the same skill group. Tier 2 Support Rep will take all steps necessary to reproduce, understand and resolve the issue.
- Technical Issues that cannot be resolved by the Tier 2 Support Rep are escalated to Tier 3. This escalation will provide a deeper layer of analysis with the possibility of escalation to QA/Development for Application issues and Escalation to Operation Services for Infrastructure issues as needed.
- Functional Issues that cannot be resolved by Tier 3 are escalated to Product Management.
- If it is an application Issue, necessary Development work will be performed, tested and a patch created.
- Issue Fix Submitted to Operations for Infrastructure issues.
- Issue Fix deployed.
- Tier 2 Support Rep confirms success of Bug Fix in addressing the problem.

- Tier 2 Support Rep contacts customer and confirms that the issue is Resolved.
- Case is closed.

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

Consequences and remedies for failure to meet response time and incident fix time will all be detailed in each individual project's scope of work document.

8.12.5 - Describe the firm's procedures and schedules for any planned downtime.

Accenture's cloud solutions built on AWS and our direct AWS IaaS and PaaS offerings have limited scheduled downtime. When necessary, we work with customers to fit scheduled downtimes into timeframes that work for our customer. Reminders can be sent and posted per a given customer's needs.

SALESFORCE

There are two types of maintenance at Salesforce: System Maintenance and Release Maintenance. System Maintenance is for sustaining the performance, reliability, security, and stability of the infrastructure supporting our services. When maintenance is scheduled, the specific timing and availability to be expected during that time will be communicated to all customers approximately one week in advance of the maintenance window upon login to Salesforce and via a posting to http://trust.salesforce.com/trust/maintenance. In the event of planned maintenance where the services will be unavailable for more than four hours, or that requires customer action in advance, Salesforce endeavors to communicate via email several months in advance. Please Note: If emergency system maintenance is required, customers may be notified less than one (1) week in advance.

Major Release Maintenance is for upgrading the services to the latest product version to deliver enhanced features and functionality. Major release dates and times are posted on http://trust.salesforce.com/trust/maintenance approximately one month before release to Sandbox instances. An email notification and blog post regarding Sandbox preview instructions is also sent approximately one month prior to upgrading Sandbox instances. Email notification of major release dates is sent one month prior to upgrading non-Sandbox instances. The Release Notes document describing the new features and functionality is posted in Help & Training one month prior to upgrading non-Sandbox instances. Final release reminders are communicated to all customers approximately one week prior via email and upon logging into Salesforce.

Major release maintenance occurs three times per year. The instance will be unavailable for up to five minutes during the release window.

Patch Releases and Emergency Releases are used to deliver scheduled and ad hoc application fixes. Patch releases are scheduled weekly and are usually deployed to instances on Tuesday, Wednesday or Thursday, with release to Asia-Pacific instances the following day. Emergency releases are conducted on an as-needed basis and can occur any day of the week. Whenever possible, patches and emergency releases are deployed during off-peak hours and without downtime.

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

Accenture's approach is to leverage the expansive infrastructure of AWS and Salesforce to greatly limit the potential impact of disasters. Accenture's would work with each customer to define specific consequences if disaster recovery metrics are not met for our cloud solutions built on AWS and our direct AWS IaaS and PaaS offerings.

SALESFORCE

Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, and backed up at the primary data center. Backups are performed daily at primary data center facility without stopping access to the application.

For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4-hour recovery point objective (RPO) and 12-hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and your Agency.

In terms of remedies, the Salesforce Service Terms incorporated as part of the End User Licensing Agreement indicate the following regarding Termination allowing customers to terminate the contract at time of renewal:

"User subscriptions will automatically renew for additional periods of one (1) year at the list price in effect at the time of renewal unless You give Your Reseller notice of termination at least 30 days prior to the end of the relevant subscription term."

8.12.7 - 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.

Accenture's cloud solutions built on AWS and our direct AWS IaaS and PaaS services have performance information posted here: Service Health Dashboard

Salesforce system status and performance information is posted here: https://status.salesforce.com/

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

The Accenture Cloud Platform provides access to real-time performance information for IaaS components that can be printed. Our cloud hosting partners have more detailed reporting for each of the services including the CloudWatch service for AWS, which includes historical, statistical, and usage reports that can be printed locally.

SALESFORCE

Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find:

- Live and historical data on system performance
- Up-to-the minute information on planned maintenance

- Phishing, malicious software, and social engineering threats
- Best security practices for your organization
- Information on how we safeguard your data

In addition to the Salesforce Trust site (http://trust.salesforce.com/trust/status) to monitor uptime and performance, your Agency will also have access to a System Overview, which will help you monitor performance and usage of your own Salesforce org. This overview includes:

- Schema - # and % of custom objects and data storage
- Business Logic - # and % of Rules, Apex triggers and classes, as well as % of code used
- License Usage
- API Usage - # and % of requests in the last 24 hours
- User Interface - # and % of custom apps, sites, flows, custom tabs and pages
- Portal Usage

The above list is of all the possible metrics that you may have in your system overview. All of these metrics can be printed locally through the user's browser.

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

All Accenture' proposed services has ability to provide on-demand deployment 24x365.

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

All services Accenture has proposed for IaaS, PaaS, and SaaS include the ability to deploy and scale up or down at any time 24x365.

8.13 (E) CLOUD SECURITY ALLIANCE

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.
a. Completion of a CSA STAR Self-Assessment. (3 points)
b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)
c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
d. Completion CSA STAR Continuous Monitoring. (5 points)"

AWS

Accenture is a corporate member of the Cloud Security Alliance (CSA) and our solutions built on AWS leverage the CSA materials for AWS as described below. AWS aligns with the CSA STAR Attestation and Certification based on third-party audits and is CSA STAR Level 2 Certification based on ISO 27001. A copy of the current completed CSA Consensus Assessments Initiative Questionnaire (CAIQ) is provided in Attachment B.

SOLUTIONS OFFERED ON AWS	SERVICE MODEL
Accenture Cloud Platform	IaaS

SOLUTIONS OFFERED ON AWS	SERVICE MODEL
Desktop as a Service	IaaS
Accenture Reach Platform	PaaS
Database as a Service	PaaS
Accenture Insights Platform	SaaS
Accenture DevOps Platform	SaaS
Accenture Virtual Assistant Platform	SaaS

Updated information on AWS services can be found at https://aws.amazon.com/compliance/csa/.

SALESFORCE

Salesforce is also a corporate member of the CSA and contributes to their research and initiatives in a variety of ways. Salesforce has completed the CSA CAIQ for the Salesforce Services, including Force.com, Analytics Cloud, Communities, Chatter, Sales Cloud and Service Cloud. A copy of the current completed CSA CAIQ and CCM is provided in Attachment B.

SOLUTIONS OFFERED ON SALESFORCE	SERVICE MODEL
Salesforce Platform	PaaS
Salesforce Service Cloud	SaaS

8.14 (E) SERVICE PROVISIONING

8.14. 1 - Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.
8.14.2 - Describe in detail the standard lead-time for provisioning your Solutions.

Accenture would work with Purchasing Entities to contract for new services in as little as a few days. Once services are contracted, the cloud principle of Elasticity means that most cloud services can easily have additional capacity or category services provisioned.

AWS

AWS uses the term “elastic” to describe the ability to scale computing resources up and down easily, with minimal friction. Elasticity helps you avoid provisioning resources up front for projects with variable consumption rates or short lifetimes. Instead of acquiring hardware, setting it up, and maintaining it to allocate resources to your applications, you use AWS to allocate resources using simple Application

Program Interface (API) calls. Elastic Load Balancing and Auto Scaling can automatically scale your AWS cloud-based resources up to meet unexpected demand, and then scale those resources down as demand decreases.

Auto Scaling

Auto Scaling allows customers to automatically scale their Amazon EC2 capacity up or down according to conditions that they define. Auto Scaling is well suited for applications that experience hourly, daily, or weekly variability in usage. Customers can automatically scale their Amazon EC2 fleet or maintain their Amazon EC2 fleet at a set size.

Auto Scaling enables customers to closely follow the demand curve for their applications, reducing the need to provision Amazon EC2 capacity in advance. For example, customers can set a condition to add new Amazon EC2 instances in increments of three instances to the Auto Scaling Group when the average CPU utilization of the Amazon EC2 fleet goes above 70 percent; and similarly, customers can set a condition to remove Amazon EC2 instances in the same increments when CPU utilization falls below 10 percent.

Often, customers may want more time to allow their fleet to stabilize before Auto Scaling adds or removes more Amazon EC2 instances. Customers can configure a cool down period for their Auto Scaling Group, which tells Auto Scaling to wait for some time after taking an action before it evaluates the conditions again. Auto Scaling enables customers to run their Amazon EC2 fleet at optimal utilization.

Elastic Load Balancing

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables customers to achieve even greater fault tolerance in their applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored. Customers can enable Elastic Load Balancing within a single Availability Zone or across multiple zones for even more consistent application performance.

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch 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, Amazon RDS database instances, custom metrics generated by applications and services, and any log files your 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 and keep applications running smoothly.

Amazon CloudWatch's metrics and alarms can work together with Auto Scaling and ELB to dynamically deploy new instances on-demand, as depicted in Figure 12.

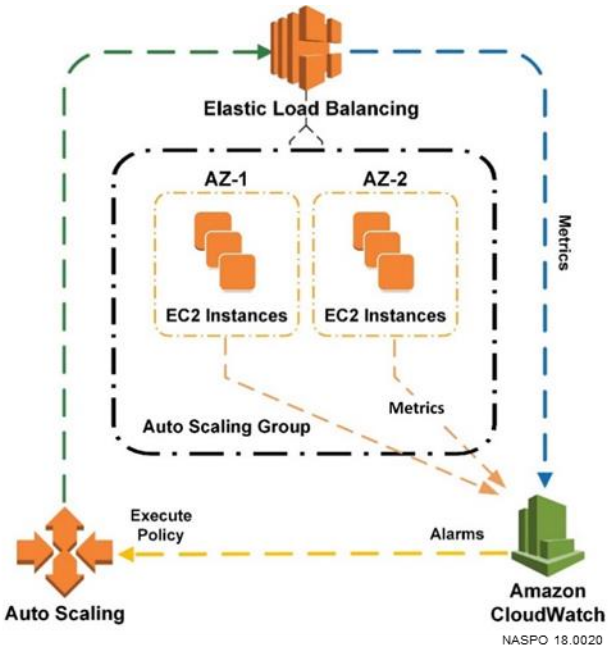


Figure 12. Amazon CloudWatch's metrics and alarms can work together with Auto Scaling and Elastic Load Balancing to dynamically deploy new instances on-demand.

SALESFORCE

Salesforce offers on-demand Platform as a Service (PaaS) and Software as a Service (SaaS). The Salesforce PaaS and SaaS offerings are subscription based and in a per user/month or user/year format billed annually with some of our products offered as total logins per month or by defined number of members billed annually.

Multi-tenancy gives applications elasticity. Force.com applications can automatically scale from one to tens of thousands of users. Processing more than three billion transactions each day, Force.com is used for large-scale deployments. Any application that runs on Force.com is automatically architected to seamlessly scale from 1 user to 100,000 users without the customer having to do anything differently.

All applications (includes mobile, offline and read-only options) and data running on Force.com are deployed to and replicated across multiple data centers in different geographies. Every application, no matter how large or small, gets the full benefits of the backup, failover, disaster recovery, and other infrastructure services required for an organization’s mission-critical applications.

8.15 (E) BACK UP AND DISASTER PLAN

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

Accenture’s solutions can apply retention periods based on legal requirements that would be requested for a specific engagement.

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

While disasters are always possible, Accenture believes the capabilities inherent in cloud environments from AWS and our other partners provide sufficient capabilities to significantly reduce any inherent risks. Accenture would leverage mitigation strategies such as data replication across Availability Zones or Regions depending on the sensitivity of the data. Below is more information on how AWS supports data retention.

AWS

AWS gives customers ownership and control over their content by design through simple, but powerful tools that allow customers to determine where their content will be stored, how it will be secured in transit or at rest, and how access to their AWS environment will be managed.

- Customers control their customer content. With AWS, customers determine where their customer content will be stored, including the type of storage and geographic region of that storage.
- When customers store content in a specific region, it is not replicated outside that region. It is the customer's responsibility to replicate content across regions if business needs require it.
- Customers can replicate and back up their customer content in more than one region, and 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.
- Customers choose the secured state of their customer content. AWS offers customers strong encryption for customer content in transit or at rest, and provide customers with the option to manage their own encryption keys.
- Clients manage access to their customer content and AWS services and resources through users, groups, permissions, and credentials that customers control.

SALESFORCE

The Salesforce service performs near real-time replication at each data center and annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center. The disaster recovery site is a 100% replica of the primary production site of capacity (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location [CP-4, CP-6, CP-7, CP-9, MP-5].

8.15.3 - 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.

Accenture's cloud solutions leverage AWS data centers including the redundancy and failover capability described below.

AWS

Amazon S3 supports data replication and versioning instead of automatic backups. You can, however, backup data stored in Amazon S3 to other AWS regions or to on-premises backup systems. Amazon S3 replicates each object across all Availability Zones within the respective region. Replication can provide data and service availability in the case of system failure, but provides no protection against accidental deletion or data integrity compromise–it replicates changes across all Availability Zones where it stores copies. Amazon S3 offers standard redundancy and reduced redundancy options, which have different durability objectives and price points.

Each Amazon EBS volume is stored as a file, and AWS creates two copies of the EBS volume for redundancy. Both copies reside in the same Availability Zone, however, so while Amazon EBS replication can survive hardware failure, it is not suitable as an availability tool for prolonged outages or disaster recovery purposes. AWS recommends that you replicate data at the application level, and/or create backups. Amazon EBS provides snapshots that capture the data stored on an Amazon EBS volume at a specific point in time. If the volume is corrupt (for example, due to system failure), or data from it is deleted, you can restore the volume from snapshots. Amazon EBS snapshots are AWS objects to which IAM users, groups, and roles can be assigned permissions, so that only authorized users can access Amazon EBS backups.

SALESFORCE

Customer Data for customers in Salesforce's Government Cloud is stored in two of our U.S. data center locations. Our service is co-located in dedicated spaces at top tier data centers. Salesforce's hardware is located inside of secure server rooms designated to Salesforce and separated by concrete walls from other data center tenants. Individual racks inside of the data center are secured with a lock. Specific racks are allocated for hardware supporting the Salesforce Government Cloud. Access to the racks supporting the Salesforce Government Cloud hardware is restricted to Qualified U.S. Citizens as described in the section above.

8.16 (E) HOSTING AND PROVISIONING

8.16.1 - Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.
8.16.2 - 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)."

The Accenture Cloud Platform (ACP) provides two methods to provision a cloud stack including the use of the Cloud Provider's console or through the ACP console explained in the below response.

Provisioning through Cloud Provider's console

The ACP's discovery engine allows you to access services and provision services through the native cloud provider console. This model provides you with consistent insight into services across cloud providers through the ACP console. It also helps you to use the native cloud provider console to leverage

new service introductions and innovations from cloud vendors immediately, helping improve speed to value.

Provisioning through the ACP Console

The ACP console contains the key information needed to effectively build and deploy applications in the cloud— including server, software, storage, network, images, and firewall details. The platform's automated, self-service blueprints enable multiple cloud services to be bundled, provisioned, and deployed from a single point of control across providers.

Control with the enterprise level governance

A single multi-cloud dashboard provides central monitoring of service usage and delivery across multiple services end private and public clouds. As a one-stop shop to request and provision pre-approved cloud services, the platform also provides policy management and approval workflow control, along with a suite of billing, chargeback, and cost analytics. This access helps make enterprise management and scaling of cloud services easier.

Below are specific provisioning capabilities provided by the AWS native console and tools.

AWS

AWS provides a broad set of services that help IT administrators, systems administrators, and developers more easily manage and monitor their resources. Using these fully managed services, customers can automatically provision, configure, and manage their AWS or on-premises resources at scale. Customers can also monitor infrastructure logs and metrics using real-time dashboards and alarms. AWS also helps customers monitor, track, and enforce compliance and security.

Resource Provisioning

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Customers can use AWS CloudFormation's sample templates or create their own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run their application.

AWS Marketplace is an online store that helps customers find, buy, and immediately start using the software and services they need to build products and run their businesses. AWS Marketplace features many software categories including databases, application servers, testing tools, monitoring tools, content management, and business intelligence. Visitors to AWS Marketplace can use 1-Click deployment to quickly launch pre-configured software and pay only for what they use, by the hour or month. AWS handles billing and payments, and software charges appear on the customers' AWS bill.

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, helps them achieve consistent

governance, and helps them meet their compliance requirements, all while enabling users to quickly deploy only the approved IT services they need.

Configuration Management

AWS OpsWorks is a configuration management service that helps customers configure and operate applications of all shapes and sizes using Chef. Customers can define the application's architecture and the specification of each component including package installation, software configuration, and resources such as storage. Customers can start from templates for common technologies like application servers and databases or build their own to perform any task that can be scripted. AWS OpsWorks includes automation to scale applications based on time or load and dynamic configuration to orchestrate changes as an environment scales.

AWS Systems Manager allows customers to centralize operational data from multiple AWS services and automate tasks across AWS resources. Customers can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. With AWS Systems Manager, customers can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. AWS Systems Manager provides a central place to view and manage AWS resources, so customers can have complete visibility and control over their operations.

Monitoring and Performance

Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, Amazon Relational Database Service (Amazon RDS) DB instances, custom metrics generated by the 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 and then use those insights to react and keep their application running smoothly.

Governance and Compliance

AWS Config is a fully managed service that provides customers with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config Rules enable customers to create rules that automatically check the configuration of AWS resources recorded by AWS Config. With AWS Config, customers can discover existing and deleted AWS resources, determine their overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

AWS CloudTrail is a web service that records AWS API calls for a customer's account and delivers log files to them. 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. With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS Cloud services (such as AWS CloudFormation). The AWS API call history

produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, helps them achieve consistent governance, and helps them meet their compliance requirements, all while enabling users to quickly deploy only the approved IT services they need.

Resource Optimization

AWS Trusted Advisor is an online resource to help customers reduce cost, increase performance, and improve security by optimizing their AWS environment. AWS Trusted Advisor provides real-time guidance to help customers provision their resources following AWS recommended practices.

SALESFORCE

Salesforce provisioning and monitoring is all managed through the Salesforce admin console. Since Salesforce offers only PaaS and SaaS services, the provision of specific server resources is not available and therefore, those sections of the question do not pertain to Salesforce.

Identity Management

Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application.

In addition, single sign-on and two-factor authentication may be used to authenticate users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication.

Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization.

Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce.

Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally, your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce.

Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product.

User Accounts

All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data. There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field Level security.

Administrator Privileges

Each customer organization typically chooses one or more of their users to serve as its organization administrator. There is no additional cost for administrator accounts; administrators are just more powerful users of the instance. The organization administrator has access to the admin interfaces in order to configure default settings, custom fields, custom reports, role-hierarchies, add new users, reset passwords, set default pick-list values, and other functions. The organization administrator logs onto the application like other users within the organization; however, they have admin privileges granted to them which provide them with this additional access.

Permission Sets

Administrators can control permission sets to create a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users' functional access without changing their profiles. For example, to give users access to a custom object, create a permission set, enable the required permissions for the object, and assign the permission set to the users. You never have to change profiles, or create a profile for a single use case. While users can have only one profile, they can have multiple permission sets.

Use permission sets to grant access among logical groupings of users, regardless of their primary job function. For example, let's say you have an Inventory custom object in your organization. Many users need "Read" access to this object and a smaller number of users need "Edit" access. To address this requirement, you can create a permission set that grants "Read" access and assign it to the appropriate users. You can then create another permission set that gives "Edit" access to the Inventory object and assign it to the smaller group of users.

Lightning Experience is the name for the all new Salesforce desktop app, with over 25 new features, built with a modern user interface and optimized for speed. By default, the "Lightning Experience User" permission is automatically enabled for all users with a standard Salesforce profile. Participating entities

can fine-tune access to Lightning Experience with custom profiles or permission sets. This can allow a participating entity to create a limited rollout to a pilot group or enable a specific team of users who can benefit from the new interface until you are ready to roll out the new user interface to your entire organization. More information on setting up Lightning Experience can be found here: http://releasenotes.docs.salesforce.com/en-us/winter16/release-notes/lex_enable_intro.htm.

Permission sets include settings for:

- Assigned apps
- Object settings
- Tab settings
- Record type settings
- Object permissions
- Field permissions
- App permissions
- Apex class access
- Visualforce page access
- System permissions
- Service providers (only if you've enabled Salesforce as an identity provider)
- Lightning Experience
- Demo Video tutorial on Permission Sets: http://salesforce.vidyard.com/watch/UFBD2u_NM12BVNhXKsSn4g

8.17 (E) TRIAL AND TESTING PERIODS (PRE- AND POST-PURCHASE)

8.17.1 - Describe your testing and training periods that your offer for your service offerings.

Many of the offerings Accenture is proposing for this contract include trial periods for testing the services and their ability to fit a customer's need. Accenture would offer these trial periods to purchasing entities. For example, AWS offers a Free Tier for many of the services for up to a 12-month period.

With Salesforce you can sign up for a free trial and/or a free developer account. Signing up for a Developer account is strongly encouraged for anyone in your organization that is interested in learning more about Salesforce administration or general capabilities of the platform. Please keep in mind that while it is possible to migrate configuration of a Developer org to a Production org, you cannot upgrade the Developer org itself to a Production org. On the other hand, a Trial org can be (and frequently is) converted into a full Production org at the end of the trial period, making it a great solution for Production Pilot projects.

8.17.2 - Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Accenture would make AWS Free Tier available to Purchasing Entities to test AWS products and services prior to purchase. The AWS Free Tier can be leveraged by customers for a 12-Month Introductory Period and is only available to new AWS customers, and is only available for 12 months following initial AWS sign-up date. Accenture has guided new customers using AWS Free Tier as a precursor to purchasing AWS services. Often, Accenture customers find AWS Free Tier is sufficient to understand how products will be integrated into their environment and as a proof of concept prior to purchase. A full list of products and services can be found at https://aws.amazon.com/free/.

See above answer to 8.17.1 for the Salesforce response.

8.17.3 - Offeror must describe what training and support it provides at no additional cost.

Accenture would build in training specific to a statement of work for a given customer based on the services that are included. In addition, each of our subcontractors includes free training available through their web sites below.

- AWS - https://www.aws.training/
- Salesforce - https://trailhead.salesforce.com

8.18 (E) INTEGRATION AND CUSTOMIZATION

8.18.1 - Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

The Accenture Cloud Platform (ACP) manages and integrates with cloud technology from a broad range of leading global public cloud providers such as Amazon Web Services, Microsoft Azure, Oracle Cloud, and the Google Cloud Platform. In addition, ACP also integrates to private clouds based on VMware and OpenStack architectures. A centralized dashboard gives organizations the control and agility to manage their business services simply, securely, and effectively across multiple clouds on demand, at speed, from a single point. This confirms an agnostic approach allowing our clients the flexibility to have vendor portability and no technology lock in.

In addition to ACP integrations, Accenture has the ability to extend our technology and business capabilities through a powerful alliance ecosystem of market leaders and innovators. Together, we provide our clients the best specialized skills and New IT solutions. Table 1 is the current list of ecosystem partners that Accenture works with.

ABB	Accelatis	ACI Worldwide	Adam Software	Adaptive Insights
ADI Strategies	Adobe Systems	AFS	Alert Logic	Alevo Inc.
Amadeus IT Group	Amazon Web Services (AWS)	Anaplan	Apigee	Appcelerator
AppDynamics	Applause	Apteligent	Apttus	Aras
Avaloq	Avaya	AvePoint	Ayasdi	BMC Software

Backbase	Basis Technology	Benefitfocus	Blu Age	Blue Prism
Box Inc.	CA Technologies	CallidusCloud	Calypso	CARTO, Inc.
CentriHealth	Chef	CipherCloud	Cisco	ClickFox
ClickSoftware	Cloudera	Coupa	CSG International	Dassault Systèmes
DataStax	Dell	Digital Asset Holdings	Docker	Dynamic Action
E2OPEN	EcoSys	Elastic Path	EMC	eMeter
Enablon	Endgame	Esri	eVision	Ferranti Computer Systems
FICO	Finastra	FirstBest	Flexera Software	FNZ
ForgeRock	Fujitsu Siemens Computers	General Electric	Genesys	GoldenSource
Good Technology	Google	Guidewire	Halliburton Landmark	HealthEdge
HireFx	Hortonworks Inc	HPE	HP Inc	Huawei
HubHead	Hybris	Hyland Software	IBM	IBS Software Services Americas
IFS	Imagine Communications	Informatica	Interactive Intelligence	Intergraph Corporation
iRise	JDA	Jive Software	Kinaxis Corp	Kony
Kronos	Liferay	Lightbend	Lombard Risk	Management Controls
Marketo	Medallia	Medidata	Micro Focus	Microsoft
MicroStrategy	Mobilize	Moven	MuleSoft	Murex
MWH Americas Inc.	nCino	NetApp	NetSuite	NewOak
Nexidia	Nimble	Nokia	Nuance	
Nutanix	Okta	Open Text Inc.	OpenLink	Opowe
Oracle	OSIsoft	Palo Alto Networks, Inc.	Paydiant	Pegasystems
Pitney Bowes Inc.	Pivotal	Predixion Software	PROS	PTAG

PTC	Pure Storage	Qlik	Quest Software	Red Hat
RichRelevance	Ripple Labs	SailPoint	Salesforce.com	SAP
SAS	ServiceMax (part of GE)	ServiceNow	ServiceSource	Siemens Enterprise Communications
Siemens PLM	SiteCore	SmartStream	SOAST	Software AG
SourceCode Technology	Space-Time Insight	Spare5 - Mighty AI	Splunk	Stibo Systems
Stibo Systems A/S	Symantec	Tableau Software	Talend	Tanium, Inc.
Teradata	Teradata Operations Inc.	Temenos	ThinkAnalytics	Thomson Reuters
TIA Technology	TIBCO	Tricentis	Veeva Systems	VenueNext
Verizon Sourcing	Verimatrix, Inc.	Vlocity	VMware	Vodafone
WCC	Webtrends	Work Market	Workday	Worksoft
Yucheng Technologies				

Table 1. Accenture's current list of Ecosystem Partners that we can integrate solutions for NASPO's Purchasing Entities.

SALESFORCE

Connecting Salesforce to an existing enterprise application is a common and frequently performed task. Integration options range from native Web Services support (APIs, outbound workflow, etc.) to import/export utilities to middleware integration via packaged connectors to toolkits for Java, .NET, and other open platforms. Our solution provides the ability to call out to virtually all common APIs, to enable synchronization, push/pull, and mash-ups with external apps/systems. Salesforce itself is based on web-service based APIs that in turn simplify access to Salesforce data from external systems. API-based integration is heavily leveraged by our customers.

The APIs are provided with the Salesforce Force.com platform to build integration interfaces with third party applications or by our integration partners to use in their connectors. Any 3rd party application that accesses your Salesforce instance via the APIs, will be subject to the same security protections that are used in your Salesforce user interface. Therefore, the 3rd party application will need to use a "granted" user in order to access the Salesforce data. These are open APIs (based on industry-standards such as REST and SOAP) that you can use to integrate Salesforce endpoints with external endpoints such as apps or enterprise integration hubs. As an example, you have the Batch and Bulk APIs used in the Data integration patterns or the SOAP and REST APIs used for UI integration patterns.

Integration Options as various Layers of a Solution

Salesforce lets you choose integration methods at different layers to optimally align with business requirements, security policies, and master data management guidelines. Specifically, a participating entity can choose how best to integrate across Security, User Interface, Business Logic and Data Integration layers. For more details on optimal design patterns for integration, see the Whitepaper "Integration Patterns and Practices" at: https://resources.docs.salesforce.com/196/latest/en-us/sfdc/pdf/integration_patterns_and_practices.pdf

Five Paths to Integration Success

Salesforce Force.com provides paths to integration success—all based on our industry-leading Web services API—and an extensive integration partner ecosystem. Integration with Salesforce Force.com means faster, simpler, and less-risky integration that doesn't break during upgrades and delivers a new level of access and agility to your existing IT investments.

1) Choose your integration middleware - Force.com is designed to work with all major integration middleware solutions. For a list of certified integration solutions, check out the Integration category in the AppExchange marketplace (https://appexchange.salesforce.com/category/integration). Here you'll find pre-built connectors and the services of numerous integration technology partners such as IBM CastIron, Informatica Software and Jitterbit.

2) Build it yourself - For building custom integrations plus maximum flexibility and choice, the Salesforce Force.com Platform supports all major development environments and tools, including .NET, Java, PHP, Ruby on Rails, and many more. Learn more from our wiki developer network at developer.force.com.

3) Find it on the AppExchange - For the easiest and fastest way to add pre-integrated functionality, check the AppExchange directory. You can integrate with 2,900+ components and applications with the click of a mouse. Learn more at appexchange.salesforce.com. Here you will find both free and pay-as-you-go licensed add-ons.

4) Connect the clouds - Harness the power of multiple clouds. Learn how to connect Salesforce Force.com with the data and content of the most popular cloud services, including Amazon Web Services, Facebook, Google AppEngine, and Twitter. For example, you can enrich your Salesforce Contacts' profiles integrating with the likes of Facebook or Twitter to create a 360-degree single view of your customers.

5) Use our native connectors - Whether you need to integrate with the most common desktop productivity tools; Microsoft Excel, Microsoft Outlook, Microsoft Word, or ERP suites from Oracle or SAP, Force.com provides proven native connectors. Salesforce applications have proven to be an excellent way to get critical data from Oracle accounting and ERP applications into the hands of a much larger customer-facing audience. Information from Oracle ERP application suites, Oracle databases, or Oracle Fusion middleware can be easily exposed within Salesforce to create innovative and effective end-to-end business processes that drive higher user adoption and result in more effective business strategies.

For more information on integration capabilities, please visit:
https://developer.salesforce.com/page/Integration

Developer toolkits

These toolkits provide the ultimate in integration flexibility and choice. The Force.com platform supports all major development environments and tools, including Java, .NET, PHP, and Ruby on Rails.

8.18.2 - Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Accenture's proposed solutions are flexible and provide the ability to configure, modify, and manage many of the parameters at the discretion of the purchasing entities. Server configurations, environments, backup and recovery, security, etc. are all highly customizable and configurable in an IaaS environment. Implementation of these customizations is dependent upon the actual requirements.

SALESFORCE

The Salesforce Platform offers a core set of technologies that not only power the Salesforce SaaS products, but also allows you to build custom apps, connect data from any system, and manage it from anywhere. The Salesforce Platform allows customers to build apps fast with just a few clicks, designed for desktop and mobile devices, all from a single canvas. The Salesforce Platform has been given top ratings by Gartner, Forrester, & Info-Tech Research. To help IT deliver apps faster, the Salesforce Platform offers a simple yet powerful set of declarative, point-and-click tools that anyone can use to achieve business goals at lightning speed. Without writing code, developers and business users alike can quickly and easily create custom apps on the Salesforce Platform with complex business logic and beautiful user interfaces designed specific to every screen. Salesforce Lightning Builder tools allows you to work in alignment with agile development methodologies as IT meet business demands faster. The Platform uses open APIs based on industry standards such as REST and SOAP to make it easy to build apps that integrate with legacy systems. For more complex applications, developers can leverage the Apex programming language. Apex is an object-oriented, on-demand language. It is like Java, with similar syntax and notation, and is strongly-typed, compiled on demand, and fully integrated into the Platform. All of the application services come right out of the box, from a powerful workflow engine to API services, integration services, authentication, event log framework, analytics, and collaboration.

Administrator Privileges

Each customer organization typically chooses one or more of their users to serve as its organization administrator. There is no additional cost for administrator accounts; administrators are just more powerful users of the instance. The organization administrator has access to the admin interfaces in order to configure default settings, custom fields, custom reports, role-hierarchies, add new users, reset passwords, set default pick-list values, and other functions. The organization administrator logs onto the application like other users within the organization; however, they have admin privileges granted to them which provide them with this additional access.

8.19 (E) MARKETING PLAN

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities."

Accenture has a long-term commitment to the Public-Sector market through a dedicated Public-Sector practice. Accenture has long maintained a dedicated practice in State and Local government as well has Higher Education. We serve all facets of the state and local government market including, administrative back office, citizen services, pensions, public safety and human services with dedicated practices in each of these areas.

We expend significant resources on research and development to develop both thought leadership and hard assets to bring our clients. This research assists our clients in modernizing their operations and delivering efficient and effective services to their citizens. Accenture's current point of view is that our clients should be moving their applications to the cloud and in many cases from those legacy applications to SaaS products. As we work with clients on these efforts one of the challenges has been client's need to rethink and redesign traditional RFPs and contracts from those suited to procure an on-premise solution to those best suited to these new types of services. NASPO's ValuePoint Cloud Solutions contract addresses these challenges. We believe this is a powerful tool forward to assist states and their political subdivisions to accelerate their move to the cloud. We believe this option for states will provide shorter procurement cycles while maintaining the open and competitive approach to vendor selection. This will be a strong addition to our thought leadership and multiple channel marketing efforts. We will seamlessly incorporate this procurement vehicle into our existing discussion with clients on why and how they should move to the cloud.

The foundation of Accenture's work is to do what is right for our clients. Accenture believes it is critical that governments move more quickly to take advantage of the efficiencies and speed to innovation of cloud technologies. Accenture has been communicating this point of view through our thought leadership as well as our marketing to the State and Local government. We have included in that communication the need to rethink procurement processes, including what is asked for in the RFP and expected contract terms. Accenture will incorporate into these points of view and related marketing materials the NASPO ValuePoint Cloud Services agreement as recommended best practice approach to addressing these issues.

Accenture understands government clients will engage partners through a competitive process and our marketing efforts begin pre-RFP to discuss with clients, Accenture skills and the deep experience we bring to a project as well as this thought leadership which we believe results in a well written RFP. This best practice thinking we bring to our clients through traditional marketing and as often by bringing in thought leaders with deep subject matter expertise and deep industry expertise to help client think through these challenges.

Accenture believes the NASPO ValuePoint Cloud Solutions contract is a best in class solution in helping governments adopt cloud as a solution for their technology needs. We will build this idea into Accenture's thought leadership and make it an integral part of our marketing to state government thorough all our teams and marketing channels.

Accenture works through several marketing channels to bring best practices to our current and future clients.

- **Published Points of View** – Accenture publishes points of view on a variety of topics including the benefits and challenges of migrating applications to the cloud. We distribute these points of view

through all these marketing channels; websites, social media, distribution at conferences and in client meetings

- **Partnership with National Associations** – Accenture is a corporate partner in several national associations including the:
  - National Governor's Association (NGA);
  - National Association of State Budget Directors (NASBO);
  - National Association of State Chief Information Officers (NASCIO);
  - National Association of State Auditor Comptroller and Treasurers (NASACT);
  - National Association of State Comptrollers (NASC);
  - National Association of State Personnel Administrators (NASPE); and,
  - National Association of State Commissioners of Administration (NASCA).

Each of these associations provides a variety of opportunities to speak at conferences, participate in webinars, publish article in newsletters, contribute to joint research, and distribute POV's. As Accenture's discusses the value of moving to the cloud and the risks and implementation approaches, use of the Cloud Solutions contract will be incorporated into these communications.

- **Client meetings** - We frequently engage in direct meetings with state government technology and business leadership. We will incorporate the Cloud Solutions contract into these discussions as a best in class solution to address these issues.
- **Social Media** - Accenture marketing team and thought leaders are active on social media. We will use these channels to share material published by NASPO ValuePoint, and our own thought leadership as well as less formal messaging on this topic.

8.20 (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. "

Accenture has evolved one of the most comprehensive frameworks in the industry to assist organizations to transform effectively into cloud-based technologies. One of the most critical elements that we have found in our experience, is the development of specific decision criteria that will help determine which application workloads are to be phased into new platforms based on a modular roadmap to confirm alignment with business objectives. For this reason, our recommendation is for NASPO to adopt an iterative framework for each participating entity to follow, in order to affect the right strategy to verify the most effective future state.

Figure 13 offers a high-level view of the Accenture methodology:

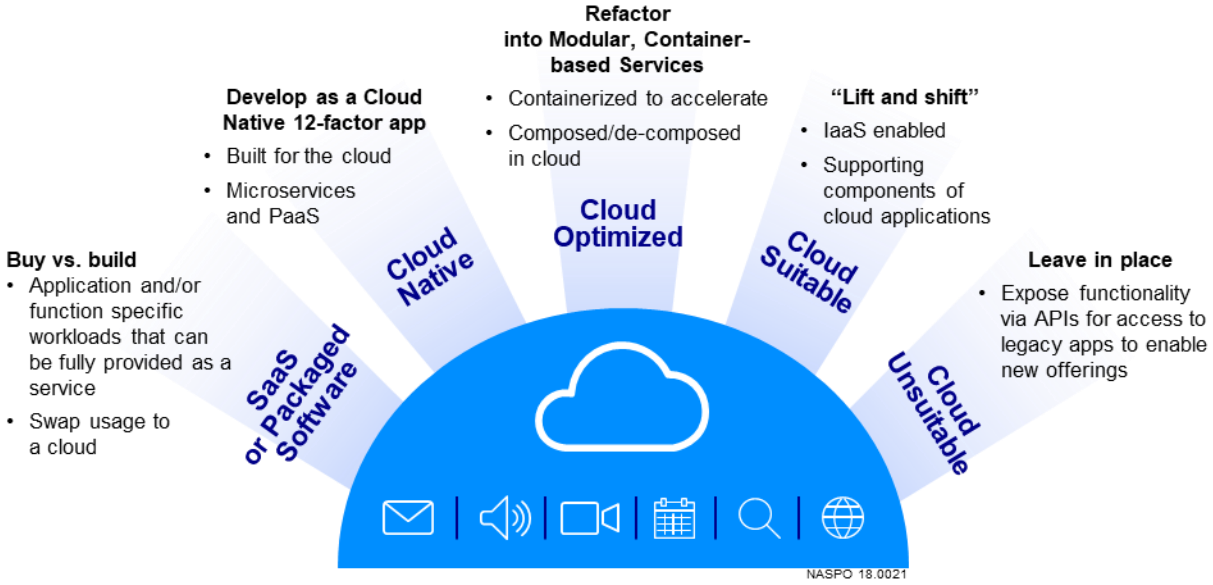


Figure 13. High-level view of the Accenture methodology

Our approach focuses first on the actual workloads in question and the proposed services and tools required to satisfy the business outcome. We first collaborate and build a consensus with each specific participating entity, to identify and categorize cloud-based workloads. We look at five workload possibilities (platform, services, tools, management, resource expertise, and costs) that need to be addressed to help align to the most suitable cloud model.

Once these workloads are agreed upon, we then can help to build a cloud framework to understand the types of services required, and with it, the associated operating model. See the framework components in Figure 14. Customer initiatives play a key factor in understanding the overall goal of IT transformation and the actual journey itself. We will work with the various agency teams to develop transformation models and decision criteria based on data analysis to develop consumption and utilization models to answer specific questions, such as:

- What is the recommended strategy for transitioning primary systems to cloud?
- What type and how much cloud automation is to be part of this transformation?
- Are the services being consumed currently going to change, and if so how, and if not do we understand why? How far is IT going to evolve and what are the possible service offerings associated with the new evolution going to be required?
- Is the participating entity looking for a managed cloud services model, a hybrid cloud services model, or a streamlined cloud consumption model with limited IT resource involvements for run and administration?
- What are the decision criteria that allow the basis for the recommendations? For example:
  - Cost considerations
  - Governance
  - Regulatory compliance
  - Security and assurance
  - Business requirements

What roles within the organization can we leverage to build a new cloud transformation team with newly identified roles, responsibilities, functions, and overall Center of Excellence (CoE) associated with an IT and/or cloud transformation RACI model? This is a very important part of the process as it will help us to not only provide a vision but will lead to helping construct a cloud transformation blueprint for all “As-a-Service” offerings.

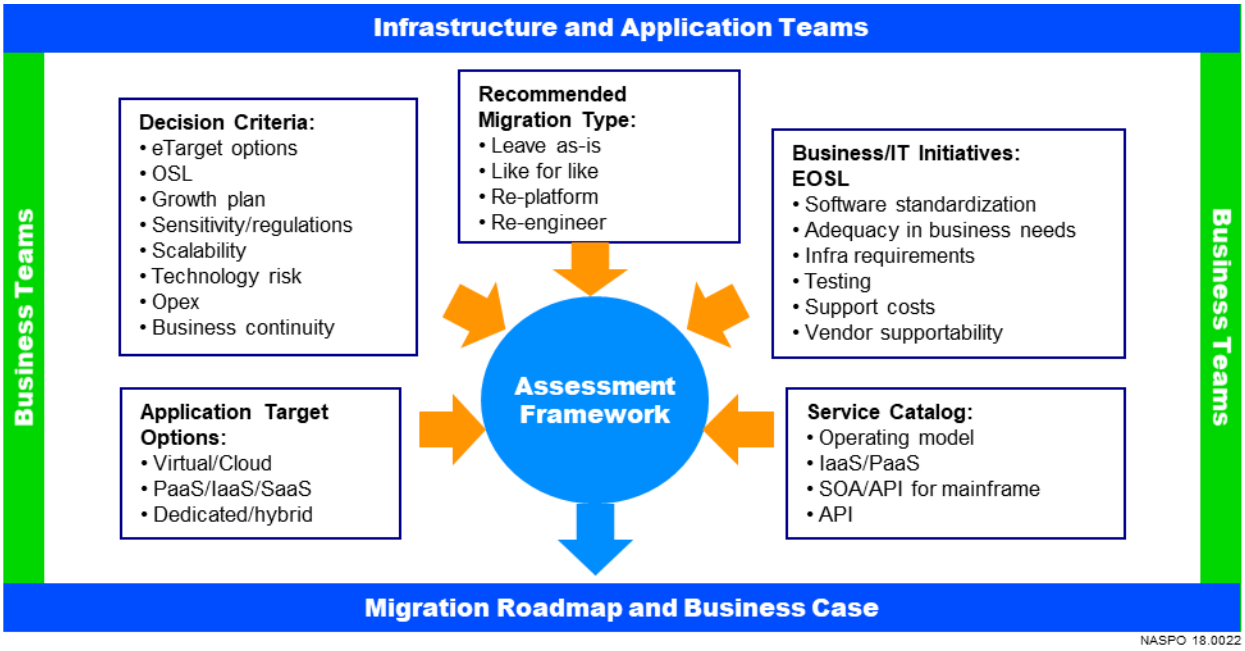


Figure 14. Accenture’s framework for determining your customized Journey to the Cloud

Using the Accenture methodology will develop the specific **Decision Criteria** along with the **Recommended Migration Types** aligned with the **Business/IT Initiatives**. The consideration of all these factors determine the **Application Target Options** and the **Service Catalog**, which details all the specific offerings that can be chosen for each specific agency.

Cloud Strategy Services

Accenture Strategy helps clients weave cloud into the fabric of their businesses and deliver everything "as a Service" or at the least take a first step in the full transformation. As illustrated in Figure 15, are the strategies that we deliver:

1. **Business Value Strategy:** Determine how the business and technology transformation can be executed, this develops the very specific cloud business case and the value realization approach validating how savings are achieved.
2. **Multi-speed Operating Model Strategy:** Define future operating models for an IT organization to function smoothly in a multi-speed environment.
3. **DevOps Strategy:** Redefine the relationship between development, operations, and business and identifies impact on tools, processes, and interaction between these teams as a result of shift to cloud adoption.
4. **Service Strategy:** Develop a solid business case, as companies need to understand what services need to be offered at different points in time.

5. **Application Strategy:** Examine which current state applications (or infrastructure needs) make the most business value sense to be fast movers.

- **Digital Resilience Strategy:** Define an organization's ability to maintain its operations in the face of an internal or external change or threat, and an organization's capacity to anticipate disruptions, and create lasting value.

Cloud Application Transformation addresses the standardization and transformation of legacy applications in preparation for migration to cloud platforms. This can include the integration of new functionality to provide the latest functions and technological advantages to the business.

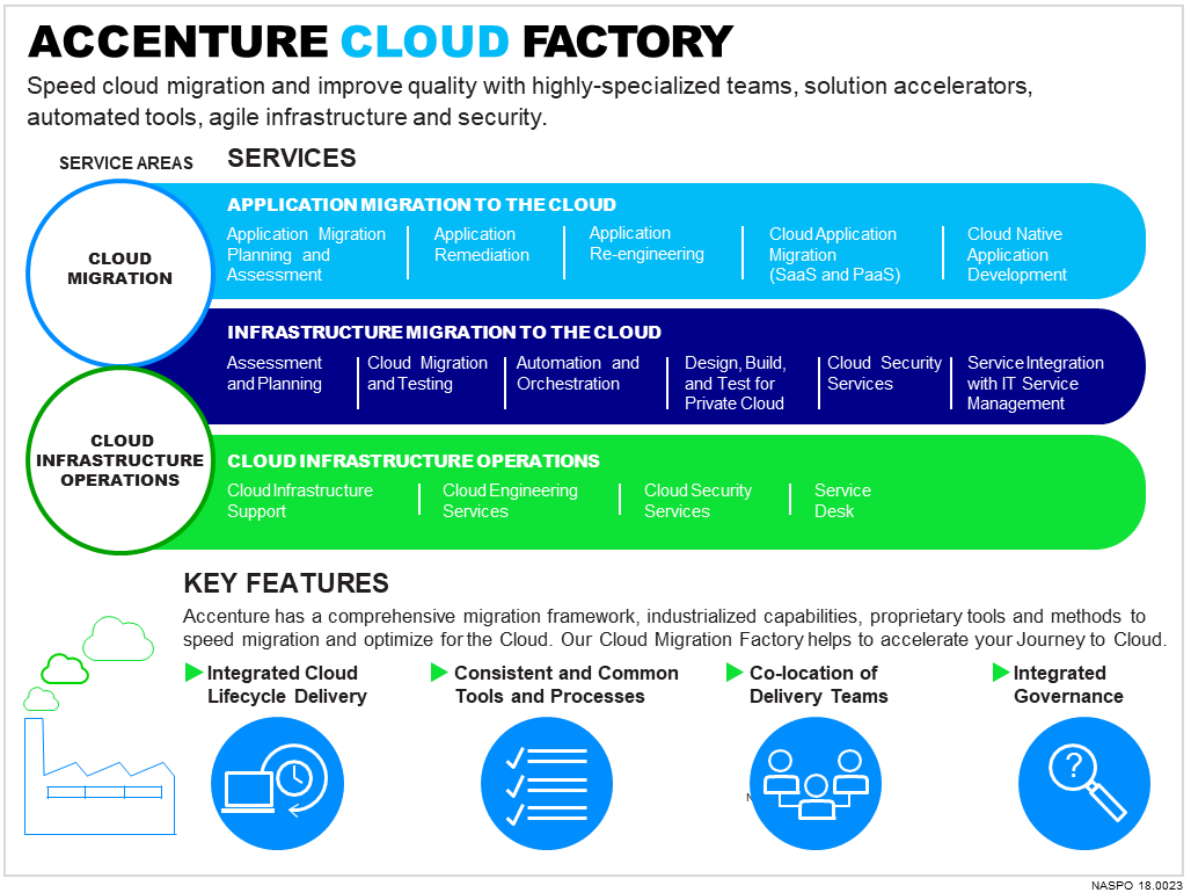


Figure 15. Accenture Strategy helps clients weave cloud into the fabric of their organizations and deliver everything "as a Service" or at the least take a first step in the full transformation.

Accenture proposes to use our Rate Card roles defined in the Cost Proposal to perform these consulting services to deliver a comprehensive and successful cloud program to purchasing entities.

8.22 (E) SUPPORTING INFRASTRUCTURE

8.22.1 - Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

Due to the nature of cloud services, there is usually no infrastructure required by the purchasing entity. However, in Hybrid Cloud environments where data is transferred between the customer's data center and the cloud provider, a Virtual Private Connection or a dedicated network connection is typically configured. Accenture would determine whether this is needed based on the specific customer requirements. The specific hardware requirements (servers, storage, etc.) would be determined by the actual Hybrid solution that was approved and implemented.

8.22.2 - If required, who will be responsible for installation of new infrastructure and who will incur those costs?

If a physical network connection or VPN is required for the engagement, the customer's network engineer would need to configure the VPN or physical network connection. The customer would also incur the costs to connect from their data center to the public cloud provider. In AWS, this configuration is provided through Amazon Direct Connect, which provides a local access point into AWS In most cases, this results in cost savings for the customer by reducing the inbound network costs from AWS.

For any Private cloud or Hybrid cloud solutions, the purchasing entity would be responsible for the acquisition and installation of any new infrastructure as well as the relocation or upgrading of existing infrastructure to support these solutions.

PROQUIRE SALES CONTRACT

This Proquire Sales Contract ("Agreement") dated _____, 20__ (the "Effective Date") is made by and between Proquire LLC ("Proquire") and _____ ("Client") and will govern Client's purchase of Products and Services (both defined below) from Proquire (each, a "Party," and collectively, the "Parties").

1. Products and Services Resale. Proquire and Proquire Affiliates (as defined below) have relationships with third party product and services vendors ("Third Party Suppliers"). Proquire resells the Third Party Supplier's products ("Products") and/or services ("Services") (collectively, "Products and Services"), which may include, but are not limited to, hardware, software, digital services, data analytics, and data processing, and Proquire may receive discounts or rebates in connection with such resale. All Products and Services are provided subject to the Third Party Supplier's applicable terms, which shall constitute an agreement between Client and the Third Party Supplier only, and not Proquire. Third Party Suppliers are independent contractors and shall not be deemed employees, agents, subcontractors, Proquire Affiliates, authorized representatives, partners or joint venturers of Proquire. A Proquire Affiliate is any entity controlling, controlled by or under common control with Proquire. As used in this definition, "control" (and variations thereof) shall mean the existing ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise.

2. Sales Quotations. Products and Services purchased or licensed by Client hereunder will be listed on sales quotation(s) issued by Proquire to Client (each, a "Sales Quotation"). Proquire will order the Products and Services specified on each Sales Quotation that has been accepted by both Client and Proquire. Client accepts a Sales Quotation by signing the Sales Quotation or by issuing a purchase order for the Products or Services listed in the Sales Quotation. Proquire accepts a Sales Quotation to the extent that Proquire orders Products or Services pursuant to such Sales Quotation. Any term, condition or proposal submitted by Client in a purchase order or otherwise (whether orally or in writing) that is inconsistent with or in addition to the applicable Sales Quotation or the terms and conditions of this Agreement will be of no force or effect, unless signed by an authorized representative of Proquire.

3. Prices and Payment. Proquire will invoice Client in the primary local currency (unless stated otherwise in the Sales Quotation). Client agrees to pay as invoiced the total purchase price for the Products and Services agreed in the Sales Quotation, plus Billable Taxes (as defined in Section 4) and applicable delivery and insurance charges. Payment in full is due within 30 days of an invoice date. Interest on any payment past due will accrue at the lower of the rate of 1.5% per month or the maximum rate allowed by law. Client will be responsible for Proquire's costs of collection for any payment default, including, but not limited to, court costs, filing fees and reasonable attorneys' fees.

4. Taxes.

a. The prices of Products and Services do not include any applicable taxes including but not limited to, sales, use, excise, value-added, business, service, goods and services, consumption, and other similar taxes or duties ("Indirect Taxes"). In addition to the purchase price, Client shall pay or reimburse Proquire for Indirect Taxes, property taxes and all other similar taxes, local fees or charges imposed by any federal, state, or local governmental entity for Products and/or Services provided under this Agreement (collectively, "Billable Taxes"), unless Client has provided Proquire with a direct pay permit or valid exemption certificate for the applicable jurisdiction. In the US only, Client's location where the Products and Services are delivered will be the location where Billable Taxes are assessed.

b. Where Proquire is required by prevailing legislation to apply Indirect Taxes in respect of any Product or Service resold by Proquire to Client, Proquire shall provide Client with a relevant invoice that specifically states the value of Indirect Taxes payable at the rate prevailing at the time of issuing valid invoice(s).

c. If Proquire has incorrectly overcharged or under charged Billable Taxes to Client, then Proquire shall correct the invoice within 60 business days of such an error being discovered and notified to Proquire, and accordingly credit to Client any Billable Taxes or charge to Client any Billable Taxes plus any applicable interest, but not penalties, charged by a taxing authority.

d. In the event that a withholding tax is payable by Client, Client shall be required to "gross up" the amount of such payment and shall pay the total amount reflected on the invoice. Client will provide to Proquire evidence that Client has remitted to the relevant authority the sum withheld within 30 days of payment to the relevant authority.

e. Each Party agrees to reimburse and hold the other Party harmless from any deficiency (including penalties and interest) relating to taxes that are the responsibility of a Party to pay under this Section. Each Party shall be responsible for taxes based on its own net income, employment taxes of its own employees, applicable social taxes, and for taxes on any property it owns or leases. Subject to the above, the price of Products and Services shall be exclusive of all such taxes, duties and levies. In the event that any taxes become chargeable or payable by Proquire or Client that have not been provided for in this Agreement, Proquire and Client will agree the relevant steps to be taken with regard to such taxes at the appropriate time. The Parties will

cooperate in good faith to minimize taxes to the extent legally permissible including, if available, acceptance of electronic delivery of software Products with no media backup.

5. Delivery and Risk of Loss. Shipment and delivery of Products and Services will be in accordance with the applicable terms and conditions of the Third Party Supplier. All orders are subject to the availability of underlying Products and Services. For hardware, title and risk of loss will each pass to Client from Proquire immediately after being transferred to Proquire from the Third Party Supplier.

6. Order Changes, Cancellations and Returns. Any order changes, cancellations or returns of Products or Services will be governed by the applicable Third Party Supplier policies. Client will be responsible for any fees, penalties or other amounts payable by Proquire or Client to any Third Party Supplier as a result of any order change, cancellation or return by Client.

7. Disclaimer of Warranty. ALL PRODUCTS AND SERVICES ARE PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, FROM PROQUIRE OR PROQUIRE AFFILIATES. CLIENT AGREES THAT THE FOREGOING WARRANTY STATEMENTS ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, AND ARE CLIENT'S SOLE AND EXCLUSIVE REMEDY. PROQUIRE, PROQUIRE AFFILIATES, AGENTS AND SUBCONTRACTORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, CONDITIONS AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, INFORMATIONAL CONTENT, SYSTEMS INTEGRATION, NON-INFRINGEMENT, INTERFERENCE WITH ENJOYMENT OR OTHERWISE ARISING OUT OF OR RELATED TO THIS AGREEMENT, INCLUDING ANY WARRANTY RELATING TO PRODUCTS OR SERVICES.

8. Limitation of Liability. This Section shall not be construed to limit any of Client's rights or remedies it may have against the applicable Third Party Supplier in an agreement between Client and such Third Party Supplier or under law. Except for each Party's confidentiality obligations, the sole liability of either Party to the other (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any and all claims in any manner related to this Agreement or the Third Party Products or Services resold will be payment of direct damages, not to exceed (in the aggregate) an amount equal to the total fees received by Proquire for the amount paid for the Product or Service giving rise to the claim. In no event will either Party be liable for any: (i) consequential, incidental, indirect, special or punitive damage, loss or expenses or business interruption, loss of data, lost business, lost profits or lost savings, or (ii) loss or claim arising out of or in connection with Client's implementation of any conclusions or recommendations made by Proquire based on, resulting from, arising out of, or otherwise related to this Agreement. Nothing in this Section 8 shall operate to limit or exclude a Party's liability for: (a) death or personal injury caused by the Party's negligence or that of its employees or agents; or (b) fraud or fraudulent misrepresentation; or (c) any other liability that cannot be limited or excluded by law.

9. Confidential Information and Personal Data. Each Party may be given access to information (in any form) that relates to the other's past, present, and future business activities and technical knowledge, which is identified by the disclosing Party as confidential information or which a reasonable person would deem to be confidential under the circumstances, excluding Personal Data ("Confidential Information"). Confidential Information may only be used by the receiving Party in connection with the Products and Services offered or purchased under this Agreement and otherwise as reasonably needed to perform its obligations under this Agreement. Proquire may disclose Confidential Information concerning Client to Third Party Suppliers only for purposes of selling or providing Products or Services to Client, including pre-sales and post-sales activities. The receiving Party agrees to protect the Confidential Information of the disclosing Party in the same manner that it protects its own similar confidential information, but in no event using less than a reasonable standard of care. Nothing in this Agreement will prohibit or limit either Party's use of information (including, but not limited to, ideas, concepts, know-how, techniques, and methodologies) (i) previously known to it without an obligation not to disclose such information, (ii) independently developed by or for it without use of the information, (iii) acquired by it from a third party who was not, to the receiver's knowledge, under an obligation not to disclose such information, or (iv) that is or becomes publicly available through no breach of this Agreement. Each Party will exercise commercially reasonable efforts not to disclose any Personal Data to the other Party and to restrict the other Party's access to its Personal Data, but if a Party is given access to the other Party's Personal Data, the receiving Party will protect such Personal Data using a reasonable standard of care against unauthorized access, use, alteration, destruction, loss or disclosure. With respect to Client Personal Data that Proquire may incidentally have access to, Client remains the data controller and Proquire shall be its data processor. The Parties shall comply with their respective obligations under all applicable laws relating to data privacy, information security or security breach notification (together, the "Data Privacy Laws"). "Personal Data" shall have the meaning given it in the Data Privacy Laws.

10. Termination and Survival. Either Party may terminate this Agreement at any time, without cause or penalty, upon 10 business days' prior written notice. However, any Sales Quotation accepted by both Parties prior to the date of termination will remain in effect and continue to be governed by the terms and conditions of this Agreement. The Parties agree that all terms and conditions of this Agreement that by their sense or nature should be deemed to survive termination of this Agreement will survive termination.

11. Governing Law and Venue. This Agreement will be governed by the substantive laws of the State of Illinois without giving effect to any choice of law rules. The United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement.

Both Parties specifically agree to submit to the exclusive jurisdiction of, and venue in, the state and federal courts in Chicago, Illinois in any dispute arising out of or relating to this Agreement.

12. Compliance with Laws. Each Party will retain responsibility for compliance with all federal, state and local laws and regulations applicable to their respective businesses. Each Party will comply with all applicable export control and economic sanctions laws and regulations, including without limitation those of the United States of America, with respect to the export or re-export of U.S.-origin or other local-origin goods, software and technical data, or the direct product thereof, and each Party agrees to abide by all such regulations in respect of all information supplied by or on behalf of the other Party.

13. Miscellaneous. The relationship between Proquire and Client is that of independent contractors and not that of employer/employee, partnership or joint venture. Except for payment obligations, neither Party will be responsible for any delays in delivery or failure to perform that may result from any circumstances beyond that Party's reasonable control. If any part of this Agreement is found by a court of competent jurisdiction to be invalid, illegal or unenforceable, all other parts will still remain in effect. Notices to be provided under this Agreement must be in writing and sent to the address set forth in the applicable purchase order, or as otherwise provided by the Parties. This Agreement and any Sales Quotation may be signed in separate counterparts each of which will be deemed an original and all of which together will be deemed to be one original, constituting the entire agreement between the Parties regarding a purchase of Products or Services from Proquire and supersedes and replaces any previous communications, representations or agreements.

14. Implementation in Other Countries. The Parties agree that Proquire's and Client's respective rights, benefits and/or obligations under this Agreement may be extended to any Proquire Affiliate and Client affiliate through a Local Country Agreement executed by such local Client affiliate and local Proquire Affiliate, provided that the addition of any such country does not violate any applicable export laws and regulations. The Parties intend that such agreement will not modify the terms of this Agreement except to the extent necessary to reflect local business conditions and legal requirements. Such local business conditions and legal requirements shall include, without limitation, the use of local currency, local law, and venue. The Parties agree that any modifications made by an amendment to this Agreement shall apply to each Local Country Agreement currently in effect or in effect in the future at the time of such amendment, and intend to update their respective local affiliates on modifications that affect local legal requirements.

The Parties hereto have executed this Agreement by their duly authorized representatives as of the Effective Date.

AGREED TO BY:		AGREED TO BY:	
Client:	_____	PROQUIRE LLC	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

ACCENTURE CLOUD PLATFORM AGREEMENT

This **ACCENTURE CLOUD PLATFORM AGREEMENT** is made and entered into as of **[**INSERT DATE**]**, ("**Effective Date**") by and between [INSERT APPROPRIATE ACCENTURE ENTITY**]**, with offices at [INSERT REGISTERED ACCENTURE ADDRESS] ("**Accenture**") and [INSERT CLIENT NAME] with offices at [INSERT REGISTERED CLIENT ADDRESS] ("**Client**"). Accenture and Client are also each referred to under this Agreement individually as a "**Party**," and together as the "**Parties**."

1 AGREEMENT STRUCTURE AND INTERPRETATION

1.1 The capitalized terms as used in this Agreement have the meanings set out in the context or in **Exhibit A** (Definitions). Section 13sets out further rules for the interpretation of this Agreement.

1.2 This Agreement sets out the general terms and conditions for the provision of ACP Services by Accenture to Client, as further defined hereunder. The specifics concerning the ACP Services to be provided by Accenture shall be detailed in a [SOW/Service Order] (a "**Service Order**"), to be executed by both Parties. Each executed Service Order constitutes a separate and binding agreement, incorporating the terms and conditions of this Agreement. This Agreement shall govern the provision and consumption of ACP Services, to the exclusion of any other terms and conditions. The terms and conditions of the [*Master Service Agreement*] entered into by the Parties on [*add date*] shall explicitly not govern or apply in any manner to the provision or consumption of ACP Services, unless otherwise stated hereunder.

1.3 If there is a conflict between the terms and conditions of this Agreement and those of any Service Order, then the following order of precedence shall apply: (i) the Service Order; (ii) any Exhibits to the Service Order and any other documents incorporated thereto by reference; (iii) the terms and conditions of this Agreement; and (iv) any Exhibits to this Agreement.

2 PROVISION OF ACP SERVICES

2.1 Subject to the terms and conditions of this Agreement, Accenture shall provide the ACP Services to Client in accordance with the executed Service Order.

2.2 The ACP Services provided by Accenture may include the following:

2.2.1 Provision of infrastructure-as-a-service, whereby Accenture shall procure server capacity in a form of virtual machines from a Cloud Vendor ("**Infrastructure Services**"), as further described in the **Exhibit 1, Infrastructure Service Description** attached to a Service Order, and as otherwise further detailed and agreed in the Service Order. *[Such Infrastructure Services may form an underlying infrastructure for other services provided by Accenture pursuant to a separate professional services agreement, such as application hosting and management services;]*

2.2.2 Provision of cloud management platform ("**CMP**"), whereby Accenture shall make its cloud management software functionality available to the Client on as-a-service basis, for the Client and its authorized End Users to access and use the cloud management platform for the purposes of requesting, provisioning, discovering and deploying cloud resources, as further described in **Exhibit 2, CMP Description** attached to a Service Order.

2.2.3 Provision of additional cloud management services ("**CMS**"), whereby Accenture shall provide additional professional services in order to assist the Client to manage the cloud infrastructure resources that the Client has procured from a third party. CMS may include, amongst other things, such services as virtual machine monitoring and/or hardening, anti-virus and other security layer implementing, operating system administration and patching, and back-up and system recovery services, as further described in **Exhibit 3, CMS Description** attached attached to a Service Order.

Infrastructure Services, CMP Services, CMS Services are, under this Agreement, referred to together as the "**ACP Services**".

2.3 Client hereby acknowledges and accepts that in relation to the Infrastructure Services, Client shall not have any direct access to the infrastructure layer (being the hypervisor layer or beyond) including any access to the administrative consoles or other any virtualised infrastructure management tools, which may have been made available to Accenture by Cloud Vendor. Instead, where so agreed in any applicable Service Order, the Client may be granted the right to administer and manage the virtual machines and server capacity procured on its behalf by Accenture as part of the Infrastructure Services solely using the CMP Service (as further described in the **Exhibit 2, CMP Services Description** attached to a Service Order).

2.4 With regard to the provision of the ACP Services, Client hereby acknowledges and agrees with the following:

2.4.1 The Infrastructure Services are provided by a Cloud Vendor, and therefore Accenture can only provide and make the Infrastructure Services available to Client subject to the terms and conditions under which the Cloud Vendor generally makes the Infrastructure Services available to public. To the extent applicable, such Cloud Vendor terms have been reflected and incorporated in the terms and conditions of this Agreement, and in the Infrastructure Services specific terms included in and attached to the Service Order.

2.4.2 That the Cloud Vendor has reserved the right to apply updates and to make such other changes to the Infrastructure Services that the Cloud Vendor deems necessary or otherwise appropriate. The Parties anticipate that in most cases such updates and changes should reflect the Cloud Vendor maintaining the Infrastructure Services to current industry standards [and therefore be beneficial to Client]. In any event, Client understands

that any changes to the Infrastructure Services by the Cloud Vendor may impact the provision of all the ACP Services.

2.4.3 [In the event where Accenture is providing CMP Services, CMS Services [and/or Transformation Services] to the Client, but not Infrastructure Services to the Client, and where the Client is procuring infrastructure services either directly from a Cloud Vendor or from a third party, the Client expressly acknowledges and agrees that Accenture does not make any representation or provide any warranty for, or be otherwise responsible for such infrastructure services provided directly by a Cloud Vendor or a third party, whether under this Agreement, implicitly or otherwise, and that in such instances the Client is solely responsible for contracting with the relevant Cloud Vendor or third party for the provision of the infrastructure services outside the scope of the ACP Services.]

2.4.4 That Accenture may also need to apply updates or make changes to the CMP Services or to the CMS Services that it is providing pursuant to any Service Order, provided always that Accenture shall not be entitled to apply such updates or other changes in a manner that would make the CMP Services or the CMS Services non-conforming with the applicable service descriptions attached to any Service Order, or otherwise materially diminish the scope or the quality of the service provided, unless such changes are necessary for Accenture to comply with any applicable laws. Accenture will use reasonable efforts to notify the Client sufficiently in advance of any planned changes to the CMP Services or to the CMS Services that have a direct impact on Client's access to or use of the relevant service.

3 CLIENT'S RIGHTS AND OBLIGATIONS

3.1 Accenture hereby grants to the Client a non-exclusive, non-transferable right during the term of the applicable Service Order to:

3.1.1 access and use the Infrastructure Services in accordance with the terms and conditions of this Agreement and the relevant Service Order, and in connection with any other services provided by Accenture pursuant to a separate professional services agreement (if applicable);

3.1.2 access and use permit its authorized End Users to remotely access and use the CMP Services in accordance with the terms and conditions of this Agreement and the relevant Service Order.

3.2 Client shall have the right to access and use the CMS Services in accordance with terms and conditions of this Agreement and the relevant Service Order, and in connection with any other services provided by Accenture pursuant to a separate professional services agreement (if applicable).

3.3 Client acknowledges and agrees that it is solely responsible for determining the suitability of the ACP Services for its business, and that the way that it accesses and uses the ACP Services complies with any applicable laws. Client is responsible for responding to any request from a third party regarding Client's use of ACP Services, such as a request to take down content under any applicable laws.

3.4 Client acknowledges and agrees that it may access and use the ACP Services solely for its own internal business purposes. Client therefore agrees that it shall not license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit the ACP Services by making them available for access or use by any third party (except End Users), including by means of operating a service bureau, outsourcing or time-sharing service.

3.5 Unless such services has been agreed to be delivered by Accenture as part of CMS Services under the applicable Service Order, Client shall be solely responsible for taking the appropriate steps to maintain security, protection, and backup of Client Data.

3.6 Client shall maintain commercially reasonable security standards for its and its End Users' use of the ACP Services, including without limitation the use of sufficiently secure passwords and regularly required password changes. Client is responsible for all use of the ACP Services by those who have access to them through Client (whether directly or indirectly), and for ensuring that its End Users maintain the confidentiality of any non-public authentication credentials associated with Client's use of the ACP Services.

3.7 Client will use good industry practice virus protection software, and other customary procedures to screen any Client Data to avoid introducing any Virus that could disrupt the proper operation of the systems used in the provision of the ACP Services. Client also agrees that it shall use all reasonable endeavors to ensure that its End Users do not upload or distribute files that contain Viruses, malicious files or other harmful code on to, or disrupt or attempts to disrupt the systems and networks used for the provision of the ACP Services. If Client learns or suspects that its End Users have introduced a Virus or such other harmful code, Client will notify Accenture and cooperate in mitigating the effects of such Virus. [OR In the event a Virus of other such code is introduced into the systems used to deliver the ACP Services due to Client's failure to use such endeavours, Client will at its cost assist Accenture in mitigating the effects of such Virus.]

3.8 Client shall be solely responsible for the acts and omissions of its End Users as if they were the acts and omissions of Client, and for ensuring that anyone who uses the ACP Services does so in accordance with the terms and conditions of this Agreement and the applicable Service Order. In particular, the Client agrees that it shall not, and that it shall ensure that its Authorized Users do not: (i) access or use the ACP Services to host or transmit any content, data or information that is illegal or which infringes any third party's rights, such as intellectual property rights or right of privacy, or which otherwise

violates any applicable laws; (ii) copy, translate, make derivative works, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code or underlying ideas or algorithms embodied in the software applications or other systems used for the provision of the ACP Services (including in the Infrastructure Services), unless expressly permitted under any applicable laws, or remove any titles or trademarks, copyrights or restricted rights notices in the systems, software and other materials used in the provision of ACP Services; or (iii) Access or use the ACP Services for the purpose of building competitive products or services by copying its features or user interface or by allowing a direct competitor of Accenture to access or use the Platform.

3.9 Client will promptly notify Accenture it becomes aware of any breach or threatened breach of the terms of this Section 3, or of any breach or threatened breach of security including any attempt by a third party to gain unauthorized access to the systems used for the provision of the ACP Services, or any other security incident relating to the ACP Services.

3.10 Client acknowledges and agrees that it is responsible for obtaining and maintaining all hardware, software, communications equipment and network connections necessary to access and use the ACP Services, and for paying any applicable third-party fees and charges incurred while accessing and using the ACP Services

4 **ACCENTURE'S RIGHTS AND OBLIGATIONS**

4.1 Accenture shall provide the ACP Services in accordance with an executed Service Order.

4.2 Accenture will use good industry standard security technologies (such as encryption, password protection and firewall protection) in providing the ACP Services. Additional security obligations, if any, shall be set forth or referenced in the applicable Service Order.

4.3 Client acknowledges and agrees that Accenture shall be permitted to monitor the Client's and its End Users' access and usage of the ACP Services limited solely for the purposes of verifying Client's compliance with the terms of this Agreement and the applicable Service Order.

4.4 Client hereby acknowledges, accepts and agrees that Accenture may have to suspend Client's and/or its Authorized Users' right to access or use all or any portion of the ACP Services, or remove any relevant Client Content as described below, where such access or use, or any Client Content: (i) poses a security risk to or may otherwise adversely impact the ACP Services; (ii) infringes or otherwise violates the rights or other interests of a third party, entails illegal or otherwise prohibited content or activities, or otherwise subjects Accenture to a potential liability; (iii) is in breach of the terms and conditions of this Agreement or the Service Order, including where Client has failed to pay to Accenture any amounts due within thirty (30) days of such payments being due; or (iv) Client has failed to respond to a claim of alleged infringement; or (v) where Accenture is required to do so under any applicable laws, or any court's or governmental body's order.

4.5 When allowed under the applicable laws and if otherwise reasonable and feasible under the circumstances (as determined by Accenture in its discretion), Accenture shall provide Client with a written notice prior to such suspension, and an opportunity to take steps to avoid any such suspension. Any suspension of Client's or its Authorized Users' right to access or use the ACP Services shall not release the Client from its obligations under this Agreement and any Service Order, including any obligation of paying the fees. Accenture's suspension right is in addition to Accenture's right to terminate this Agreement or any Service Order pursuant to Section 11.

5 **CLIENT DATA**

5.1 Client (and Client's licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to the Client Data. Except as provided in this Agreement, Accenture obtains no rights under this Agreement, express or implied, to Client Data.

5.2 Client shall be responsible for entering its Client Data into the ACP Services and Client shall be responsible for the Client Data generated through the use of the ACP Services.

5.3 Client acknowledges and agrees that it is solely responsible for the content of all Client Data, and for complying with Applicable Law relating to the Client Data, including without limitation all applicable data privacy and protection laws and regulations. Client will secure and maintain all rights in Client Data necessary for Accenture to provide the ACP Services to Client, without violating the rights of any third party or otherwise obligating Accenture to Client or to any third party. Client will obtain all required consents from third parties under applicable privacy and data protection laws before providing personal information to Accenture. As and to the extent required by law, Client shall also notify the individual Users of the ACP Services that their data may be disclosed to law enforcement or other governmental authorities, and Client shall obtain the End Users' consent to the same.

5.4 Accenture assumes no obligations with respect to Client Data, other than as expressly set forth in this Agreement, or as required by applicable laws.

5.5 Client authorizes Accenture to host, process, store and transfer its personal data in accordance with the applicable data protection laws and regulations, and any data processing provisions incorporated in or referred to in the applicable Service Order. Any processing of personal information contained in the Client Data by Accenture, will be undertaken by Accenture as a data processor acting on Client's behalf, and in accordance with instructions received from Client. Client also consents to the processing of personal information by Accenture, Cloud Vendors and subcontractors, as required to perform the

ACP Services. Client may choose to provide personal information to Accenture on behalf of third parties (including Client contacts, resellers, distributors, administrators, and employees) as part of this agreement.

5.6 Client grants to Accenture the nonexclusive right to host, store, process and transfer the Client Data (including any personal data, where applicable) solely for the purposes of and only to the extent necessary for Accenture to provide the ACP Services and as otherwise set forth in the Agreement.

5.7 Client will be responsible for providing adequate notification to and obtaining any necessary consent from data subjects in order to include any personal information within the Client Data hosted on ACP Services, including securing Accenture the right to use Client Data, as anticipated under this Agreement and the applicable Service Order.

5.8 Accenture will not disclose Client Data to any third party except: (i) to an Accenture subcontractor; (ii) as required by applicable laws, pursuant to a court order or appropriately authorized regulatory body or law enforcement agency; (iii) with Client's written consent; and/or (iv) as necessary for Accenture to establish, defend or exercise its legal rights under this Attachment and applicable laws.

5.9 Client shall have the ability to access its Client Data hosted over the ACP Services at any time during the Term set forth in the applicable Service Order. Client may export and retrieve its Client Data during the said Term, which will be subject to technical limitations caused by factors such as (i) the size of Client's instance of the ACP Services; and (ii) the frequency and/or timing of the export and retrieval.

5.10 Client acknowledges and agrees that Accenture does not control the transfer of data over the internet or a public telecommunications network and that accordingly the Accenture's obligations set forth in this Agreement and in the Service Order shall not apply to Client Data that is in transit over such networks.

6 **FEES, PAYMENTS AND TAXES**

6.1 Client shall pay the fees specified in the applicable Service Order. Fees are stated exclusive of all applicable duties, tariffs, and taxes. Unless otherwise specified in a Schedule, fees will be due and payable within thirty (30) days of Accenture's invoice. Late payments that are not the subject of a good faith dispute are subject to an interest charge, which is the lesser of: (a) one and one-half percent (1.5%) per month, or (b) the maximum legal rate.

6.2 Client will provide any information reasonably requested by Accenture to determine whether Accenture is obligated to collect VAT and sales tax from Client, including Client's VAT and sales tax identification number. If Client are legally entitled to an exemption from any sales, use, or similar transaction tax, Client are responsible for providing Accenture with legally-sufficient tax exemption certificates for each taxing jurisdiction. Accenture will apply the tax exemption certificates to charges under Client's accounts occurring after the date Accenture receives the tax exemption certificates. If any deduction or withholding is required by applicable law, Client will notify Accenture and will pay any additional amounts necessary to ensure that the net amount that Accenture receives, after any deduction and withholding, equals the amount Accenture would have received if no deduction or withholding had been required. Additionally, Client will provide Accenture with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

6.3 Client will be responsible for the payment of all taxes in connection with this Agreement including, but not limited to, sales, use, excise, value-added, business, service, goods and services, consumption, withholding, and other similar taxes or duties, including taxes incurred on transactions between and among Accenture, its Affiliates, and third party subcontractors. Client will reimburse Accenture for any deficiency relating to taxes that are Client's responsibility under this Agreement. Each Party will be responsible for its own income taxes, employment taxes, and property taxes. The Parties will cooperate in good faith to minimize taxes to the extent legally permissible. Each Party will provide to the other Party any resale exemption, multiple points of use certificates, treaty certification and other exemption information reasonably requested by the other Party.

6.4 All amounts payable under this Agreement will be made without set-off or counterclaim, and without any deduction or withholding.

7 **INTELLECTUAL PROPERTY RIGHTS**

7.1 Accenture (and its licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to the systems, software and other content and materials used in the provision of the ACP Services. In addition, Client agrees that Accenture (and its licensors, where applicable) will own all right, title and interest in and to any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Client or any other Party relating to the ACP Services, and Client hereby assigns any intellectual property rights in such items to Accenture. The Accenture name, the Accenture logo, and the product names associated with the ACP Services are trademarks of Accenture or third parties, and no right or license is granted to Client to use them.

8 **WARRANTIES AND EXCLUSIONS**

8.1 Accenture warrants that the ACP Services provided to the Client pursuant to this Agreement will comply in all material respects with the Services Descriptions attached to the applicable Service Order.

8.2 **Exclusions.** The aforesaid warranty shall however not apply where; (i) any problems have been caused by accident, abuse or where the Client's or its End Users' access or use of the ACP Services is not in accordance with this Agreement, the relevant Service Order (or any Exhibits to the aforesaid) or with Accenture's instructions; (ii) modification or alteration of the ACP Services or any systems, software or other content or materials embodied therein is made by any Party other than Accenture; or (iii) the ACP Services are being provided free of charge, or as a trial, pre-release or as a beta release.

8.3 In such event, Accenture will use commercially reasonable efforts to correct any such failure. In the event Accenture is unable to correct such failure by exercising commercially reasonable efforts for a reasonable period of time, either Party may terminate the relevant Service Order concerning the non-conforming ACP Service(s) on written notice to the other Party in which case as Client's sole and exclusive remedy, Accenture will provide a pro-rated refund of any pre-paid Fees for periods after the effective date of termination.

8.4 **Disclaimer.** EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 8, ACCENTURE, ITS AFFILIATES AND ITS LICENSORS MAKE NO REPRESENTATIONS AND PROVIDE NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE ACP SERVICES OR ANY THE THIRD PARTY COMPONENTS OR CONTENT EMBODIED THEREIN, INCLUDING ANY WARRANTY THAT THE ACP SERVICES WILL BE UNINTERUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING CLIENT DATA OR THIRD PARTY COMPONENTS OR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED, AND 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. EACH PARTY, ITS AFFILIATES AND ITS LICENSORS DISCLAIM ALL, AND THE OTHER PARTY AGREES THAT IT IS NOT ENTITLED TO, ANY EQUITABLE OR IMPLIED INDEMNITIES. THESE DISCLAIMERS SHALL ONLY APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW.

8.5 **High Risk Activities.** Accenture, on behalf of itself and its suppliers, specifically disclaims any express or implied warranty of fitness of the ACP Services for High Risk Activities.

9 **THIRD PARTY CLAIMS**

9.1 Subject to the limitations in Section 10, Accenture will defend (at its sole expense) Client and Client's Affiliates against any claims brought against Client by any third party (that is not an Affiliate of Client) alleging that Client's use of the ACP Services, in accordance with the terms and conditions of the Agreement and the applicable Service Order, constitutes a direct infringement of a patent issued as of the Effective Date, copyright, or trade secret of any third party enforceable in the United States. Accenture will only be obliged to pay the amount of any damages finally awarded against Client or the amount of any settlement agreed by Accenture.

9.2 Accenture will have no obligations or liability under Section 9.1 for any claims arising from:

- 9.2.1 Client Data;
- 9.2.2 Client's or any End User's use of the ACP Services after Accenture has notified Client, in accordance with this Agreement, to discontinue such use and Client have been afforded a reasonable opportunity to discontinue such use;
- 9.2.3 any unauthorized modification or unauthorized use of the ACP Services where infringement or misappropriation would not have occurred but for such unauthorized modification or unauthorized use;
- 9.2.4 any use of the ACP Services, or any other act, by Client or an End User, that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for the breach;
- 9.2.5 any adjudicated claim of wilful infringement directed at anyone other than Accenture and its Affiliates;
- 9.2.6 any combination(s) of the ACP Services with any other product, service, software, content, data or method not supplied by Accenture; or a free (no fee) or trial licenses of the ACP Services.

9.3 If any portion of the ACP Services are alleged to infringe any third party Intellectual Property Rights, Accenture may choose (at its election and expense) to: (a) procure the rights to use the item alleged to be infringing; (b) replace the alleged infringing portion with a non-infringing equivalent; or (c) modify the alleged infringing portion to make it non-infringing while still providing substantially the same level of functionality. If Accenture determines the actions from 9.3 (a) to (c) are not commercially reasonable, Accenture may immediately terminate Client's access to the ACP Service(s).

9.4 Client shall defend (at its sole expense) Accenture and its Affiliates and licensors against claims brought against Accenture by any third party (that is not an Affiliate of Accenture) arising from or related to (i) any use of ACP Services by Client or its End Users in violation of any applicable law or regulation; or (ii) any allegation that the Client Data violates, infringes or misappropriates the rights of a third party; (iii) Client's or its End Users' use of the ACP Services or other act in violation of this Agreement or the relevant Service Order; or (iv) Client's or any End User's engaging in High Risk Activities The foregoing shall apply regardless of whether such damage is caused by the conduct of Client and/or its End Users or by the conduct of a third party using Client's access credentials where Client has negligently made the credentials available or chosen

credentials that are easy to hack into. Client will only be obliged to pay the amount of any damages finally awarded against Accenture or the amount of any settlement agreed by Client.

9.5 Client will have no obligations of liability under Section 9.4 for any claims arising from:

9.5.1 the Client Data after Client have notified Accenture, in accordance with the terms of this Agreement, to delete the Client Data from the ACP Services and Accenture has been afforded a reasonable opportunity to do so;

9.5.2 any unauthorized access or use of the Client Data by Accenture that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for such breach; or

9.5.3 adjudicated claim of willful infringement directed at Accenture.

9.6 In connection with any third party claims pursuant to Section 9.1 and 9.4, the indemnified Party will (a) give the indemnifying Party prompt written notice of the claim; (b) reasonably cooperate with the indemnifying Party (at the indemnifying Party's expense) in connection with the defense and settlement of such claim, and (c) grant the indemnifying Party sole control of the defense and settlement of the claim, except that the indemnifying Party may not consent to the entry of any judgment or enter into any settlement with respect to the claim without the indemnified Party's prior written consent unless the settlement or judgment is purely financial, is paid entirely by the indemnifying Party, is confidential, does not require the indemnified Party to admit to any fault of wrongdoing, and fully releases the indemnified Party from any and all further claims or causes of action relating to the subject matter of the claim. The non-controlling Party may, at its expense, participate in the defense and settlement of the claim with counsel of its own choosing. In the event that the indemnifying Party fails to assume control within thirty (30) days of written notice of the claim, the indemnified Party may assume control of the defense of the claim

9.7 **Exclusive Remedy**. SECTION 9.1 CONSTITUTES CLIENT'S SOLE AND EXCLUSIVE REMEDY AND ACCENTURE'S (AND ITS AFFILIATES') ENTIRE OBLIGATION TO CLIENT WITH RESPECT TO ANY CLAIM THAT THE ACP SERVICE(S) INFRINGES OR MISAPPROPRIATES THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

10 **LIMITATION OF LIABILITY**

10.1 Under this Agreement, each Party's maximum, aggregate liability to the other is limited to direct damages finally awarded in an amount not exceeding the amount(s) Client was required to pay for the applicable ACP Services during the term of this Agreement, subject to the following:

10.2 For each ACP Service, Accenture's maximum liability to Client for any incident giving rise to a claim will not exceed the amount that Client has paid for the ACP Service in question having caused the claim during the 12 months before the incident; provided that in no event will Accenture's aggregate liability for any and all claims relating to the ACP Services exceed the total amount paid for the same ACP Services during the term of this Agreement.

10.3 **Exceptions.** THE LIMITS OF LIABILITY IN THIS SECTION APPLY TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, BUT DO NOT APPLY TO: (I) THE PARTIES' OBLIGATIONS UNDER SECTION 8; (II) VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; AND (III) ACCENTURE'S RIGHT TO COLLECT UNPAID FEES DUE HEREUNDER.

10.4 **Exclusions.** TO THE EXTENT PERMITTED BY LAW NEITHER PARTY NOR ANY OF EITHER PARTY'S RESPECTIVE AFFILIATES WILL BE LIABLE TO THE OTHER PARTY, , HOWEVER CAUSED OR ON ANY THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES; LOSS OF USE, BUSINESS INTERRUPTION, LOSS OF PROFITS OR SAVINGS, LOSS OF BUSINESS INFORMATION, REVENUES, OR GOODWILL; UNAVAILABILITY OF ANY OR ALL OF THE ACP SERVICES; INVESTMENTS, EXPENDITURES OR COMMITMENTS RELATED TO USE OF OR ACCESS TO THE ACP SERVICES; COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; UNAUTHORIZED ACCESS TO, COMPROMISE, ALTERATION OR LOSS OF CLIENT DATA OR BUSINESS INFORMATION; OR COST OF REPLACEMENT OR RESTORATION OF ANY LOST OR ALTERED CLIENT DATA.

10.5 The Parties acknowledge that the limitations on liability set out in this Section 10 are essential terms of this Agreement and the Parties would not have entered this Agreement without them.

10.6 No action, regardless of form, arising out of this Agreement may be brought by Client more than two (2) years after Client knew or should have known of the event which gave rise to the cause of action.

11 **TERM AND TERMINATION**

11.1 The term of this Agreement will commence on the Effective Date and will continue until terminated by either Party pursuant to this Section 11 (the "**Term**"). The term of any Service Order shall be agreed in the Service Order itself, and the terms and conditions of this Agreement shall survive and remain in force to govern any Service Order the term of which exceeds any termination of Agreement.

11.2 Either Party may terminate this Agreement for convenience upon ninety (90) days written notice to the other Party.

11.3 Either Party may terminate this Agreement and/or any Service Order upon written notice with immediate effect if the other Party ceases its business operations or becomes subject to insolvency proceedings, and the proceedings are not

dismissed within ninety (90) days, or otherwise becomes generally unable to meet its obligations under this Agreement and/or the Service Order.

11.4 In addition to any other remedies that a Party may have at Law, in equity, or under this Agreement, a Party may terminate this Agreement and/or any Service Order upon [thirty(30)] days' advance written notice to the other Party if the other Party commits any material breach of this Agreement and/or any Service Order and fails to cure such default (if curable) within the [thirty (30)] day period, including if there has been any such act or omission by Client or any End User that has given Accenture the right to suspend the provision of ACP Services in accordance with Section 2.5.

11.5 Accenture may also terminate this Agreement and/or any Service Order upon [ninety (90)] days' notice to Client (i) in the event where the underlying contract between Accenture and the Cloud Vendor concerning the provision of Infrastructure Services terminates, or (ii) if termination of the Agreement and/or any Service Order is necessary to comply with applicable law or binding requests of governmental entities.

11.6 Upon the effective date of expiration or termination of a Service Order, Accenture shall immediately cease Client's and its End Users' access to and use of the ACP Services.

11.7 Client shall have the ability to access and extract Client Data for a period of ninety (90) days after the expiration of termination of the applicable Service Order. Accenture will procure that the Cloud Vendor will retain the Client Data for the said time period, during which Client will cover the costs of the data storage unless other agreed in the Service Order. After the said period, all the Client Data will be deleted.

11.8 If so mutually agreed in the Service Order, Accenture shall provide to Client reasonable co-operation and assistance to facilitate the orderly wind down of the usage of the ACP Services and/or to assist Client to transition to another provider. Client will pay Accenture for such assistance at Accenture's then-current time and materials rates for the applicable services or as otherwise mutually agreed by Client and Accenture. If the termination results from a breach of this Agreement by Client, Accenture may invoice Client in advance for all transition assistance services and, if so invoiced, Client will pay in advance.

12 CONFIDENTIALITY

12.1 Each Party agrees that it will, (a) except as set forth in Section 12.2, not disclose, publish or communicate the other Party's Confidential Information to any third party, and (b) use and disclose the other Party's Confidential Information only for purposes of the Parties' business relationship with each other as contemplated by this Agreement. Each Party agrees to take reasonable steps to protect the other's Confidential Information, provided that these steps must be at least as protective as those the Party takes to protect its own Confidential Information of similar nature, but in any event no less than a reasonable standard of care.

12.2 Each Party may disclose the other Party's Confidential Information to its Affiliates, employees, contractors, licensors and agents who: (a) have a need to know it for purposes contemplated by this Agreement, and (b) are legally bound to protect the Confidential Information on terms no less protective than the terms of this Agreement.

12.3 This Section 12 will not apply to any information that either Party can demonstrate: (a) was at the time of disclosure or that has become thereafter published or otherwise becomes part of the public domain through no fault of the receiving Party; (c) was in the possession of the receiving Party at the time of disclosure to it and was not the subject of a pre-existing confidentiality obligation; (d) was received after disclosure to it from a third party who had a lawful right to disclose such information (without corresponding confidentiality obligations) to it; or (e) was independently developed by the receiving Party without use of the Confidential Information of the disclosing Party.

12.4 The receiving Party will not be considered to have breached its obligations under this Section 12 for disclosing Confidential Information of the disclosing Party to the extent required to satisfy any legal requirement of a competent governmental or regulatory authority, provided that promptly upon receiving any such request and to the extent that it may legally do so, the receiving Party: (i) advises the disclosing Party prior to making such disclosure in order that the disclosing Party may object to such disclosure or take any other action that it considers appropriate to protect the Confidential Information and; (ii) takes actions necessary to minimize any disclosure to only that necessary to satisfy any legal requirement of a competent governmental or regulatory authority (including through redaction of sensitive commercial information, where legally permissible).

12.5 Any reproduction of any Confidential Information of the other Party shall remain the property of the Disclosing Party, and the disclosing Party may, at any time including on termination or expiration of this Agreement, request the receiving Party to return, destroy or delete (and confirm the destruction or deletion of the same) as instructed (in such a manner that it cannot be recovered) all Confidential Information of the disclosing Party in the receiving Party's possession or control. Notwithstanding the foregoing, each Party may archive all copies of Confidential Information that it is required to retain to comply with law and its other record-keeping requirements.

12.6 Client shall not disclose the terms and conditions of the Agreement or the pricing contained herein to any third party unless otherwise agreed by the Parties. Neither Party shall use the name of the other Party in publicity, advertising, or similar activity, without the prior written consent of the other Party. Notwithstanding the aforesaid, Client acknowledges and agrees that Accenture may provide information regarding Client's purchase, use and consumption of Cloud Vendor

Solution, and the related terms, to the relevant Cloud Vendor, subject to obligations of confidentiality with the Cloud Vendor.

13 **ADDITIONAL TERMS**

13.1 **Compliance with Export Control Laws.** Each Party will comply with all export control and economic sanctions laws applicable to its performance under this Agreement. Client agrees that Client will and will procure that Authorized Users do not use the ACP Services in or in relation to any activities involving a country subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria or the Crimea region of Ukraine), or involving a Party in violation of such applicable trade control laws, or that require government authorization, without first obtaining the informed consent of Accenture and the required authorization. For the avoidance of doubt, Client shall not grant access to the ACP Services to any individual, entity or organization which is subject to trade sanctions or embargos by the United States or any applicable jurisdiction, including any individual, entity or organization which is listed on the OFAC Specially Designated Nationals List from time to time.

13.2 **Notices**. Unless expressly stated otherwise in this Agreement, all notices under this Agreement must be in writing and must be delivered personally, sent by certified mail (return receipt requested); or sent by express courier (with confirmation of delivery). The notice will be deemed given and will be effective upon receipt: (a) when it is delivered to a Party personally; (b) upon receipt if sent certified mail, return receipt requested; or (c) when delivered by a nationally recognized overnight courier service such as FedEx (with confirmation of delivery). Any notice by email will only be allowed in the particular Sections of this Agreement that expressly permit it. All notices must be addressed to the other Party at the address set forth in the preamble above. Either Party may designate a different address by giving ten (10) days' written notice to the other Party in accordance with this Agreement. A copy of any notice under the terms of this Agreement (except for invoices and other routine correspondence) will be forwarded to: Accenture LLP, Legal – General Counsel, 161 North Clark Street, Chicago, Illinois 60601. Such copy will not constitute effective notice. All communications and notices to be made or given pursuant to this Agreement must be in the English language.

13.3 **Governing Law and Jurisdiction**. The laws of the State of Illinois and federal laws of the United States will govern the construction, validity and operation of this Agreement and the performance of all obligations hereunder without regard for Illinois' choice of law provisions. The courts of Chicago, Illinois shall have exclusive jurisdiction in relation to any dispute or matter arising under or in connection with this Agreement.

13.4 **Force Majeure**. Other than Client's obligation to pay Accenture pursuant to this Agreement and any Service Order, neither Party will be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond its reasonable control, including but not limited to electrical or power outage, utilities or telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war, or labour disputes with its or its affiliates' employees, industrial disturbances.

13.5 **Survival**. The provisions of Sections 6, 7, 10, 11, 12 and 13, and any other Sections which by their nature are intended to survive, will survive the termination or expiration of this Agreement.

13.6 **Assignment**. Client may not assign this Agreement or delegate or sublicense any of Client's rights or obligations hereunder, including by operation of law, without the prior written consent of Accenture and any attempt to do so in violation of this provision will be null and *void*. This Agreement will be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns. Accenture may however subcontract all or part of its obligations under this Attachment to Accenture Affiliates or Cloud Vendor(s).

13.7 **Variation**. Except as otherwise expressly provided to the contrary in this Agreement, this Agreement may only be changed, modified or expanded by a writing signed by both Parties.

13.8 **No waiver**. No delay, neglect or forbearance on the part of either Party in enforcing against the other any term or condition of this Agreement will be deemed to be a waiver nor will it in any way prejudice any right of that Party under this Agreement nor will any single or partial exercise of any right preclude any other or further exercise of these rights or any other right.

13.9 **Severability**. The invalidity or unenforceability of any provision of this Agreement will not affect the validity or enforceability of any other provision hereof and it is the intent and agreement of the Parties that this Agreement will be deemed amended by modifying such provision to the extent necessary to render it valid, legal and enforceable while preserving its intent or, if such modification is not possible, by substituting another provision that is legal and enforceable and that achieves the same objective. The Parties agree that any principle of construction or rule of law that provides that an agreement will be construed against the drafter will not apply to this Agreement.

13.10 **Entire Agreement**. This Agreement, along with any Service Orders, attachments, exhibits, Attachments or referenced documents or agreements attached hereto from time to time, contains the entire Agreement between the Parties with respect to the matters specified herein and supersedes all prior or contemporaneous representations, understandings,

agreements or communications between Accenture and Client, whether written or verbal, regarding the subject matter of this Agreement.

13.11 **Relationship of the Parties**. Nothing in this Agreement will be deemed to create a joint venture, partnership, or agency relationship between the Parties or be deemed to authorize either Party to incur any liabilities or obligations on behalf of, or in the name of, the other.

13.12 **Third Party Rights**. Accenture's licensors are third party beneficiaries hereunder. This Agreement does not otherwise create any third party beneficiary rights, and in particular it is agreed that Client's End Users are not third party beneficiaries. Accenture and Client are independent contractors.

13.13 **U.S. Government Rights**. The ACP Services are provided to the U.S. Government as "commercial items" and "commercial computer software," "commercial computer software documentation," and "technical data" with the same rights and restrictions generally applicable to the ACP Services. If Client is using the Service Offerings on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Client will immediately discontinue Client's use of the Service Offerings with respect to the offending use. The terms "commercial item" and "commercial computer software," "commercial computer software documentation," and "technical data" are defined in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

13.14 **Third Party Software, Products or Services**. Accenture or Cloud Vendor may make non-Cloud Vendor products or services available to Client through the use of the ACP Services. If Client installs or uses any non-Cloud Vendor products or services, Client may not do so in any way that would subject Cloud Vendor's or Accenture's intellectual property to obligations beyond those expressly included in this Agreement. For Client's convenience, Accenture may include charges for the non-Cloud Vendor product or services as part of Client's bill for the ACP Services. Accenture, however, assumes no responsibility or liability whatsoever for the non-Cloud Vendor product or service. Client is solely responsible for any non-Cloud Vendor product or service that it installs or uses with the ACP Services. Accenture will not be responsible for any obligations set forth in any separate license or other agreement to which Accenture is not a party and that may apply to the Client Data or any portion thereof. Client will secure the necessary rights to ensure that the Client Data may be hosted by Accenture and Cloud Vendor to provide the ACP Services under the terms of this Agreement without subjecting Accenture or Cloud Vendor or their respective intellectual property to any other obligations of Client or any third party.

13.15 **Existing Agreements**. This Agreement is separate from any obligations, rights, or requirements contained in any existing master services agreement, professional services agreement, consulting services agreement, outsourcing agreement, or related agreements ("**Existing Agreements**") between the Parties. Any Existing Agreement will not apply to the products and services that are the subject of this Agreement, and this Agreement expressly overrides any conflicting statements in any Existing Agreement.

13.16 **Counterparts.** This Agreement may be executed in any number of counterparts and executed by facsimile or by other electronic communication as agreed upon by the Parties, such execution to be considered an original for all purposes, and all of which together will constitute one and the same instrument, notwithstanding that the Parties may not both be signatories to the original or same counterpart.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorised representatives and caused it to be effective as of the date first written above.

ACCENTURE:	**Client:** _____
BY:_____	BY:_____
PRINTED NAME: _____	PRINTED NAME: _____
TITLE: _____	TITLE: _____
DATE:_____	DATE: _____

EXHIBIT A
DEFINITIONS

"**ACP Services**" has the meaning given to it in Section 2.2;
"**Agreement**" means this Accenture ACP Services Agreement, any exhibits attached hereto and any other documents incorporated hereto by reference, together with any amendments hereto duly executed by the Parties;
"**Affiliate**" of a Party means any entity, whether incorporated or not, that is Controlled by, Controls, or is under common Control with such Party. "Control" means the ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise;
"**Cloud Vendor**" means the relevant cloud service provider, providing the Infrastructure Services (as defined in Section 2.2.1), as further identified in the relevant Service Order;
"**Client Data**" means any content, materials, data and information that Client or its End Users enter into a ACP Services or Client-specific data that is derived from Client's use of the ACP Services (e.g. Client-specific reports), as long as such output data is not a component of the ACP Services itself or furnished by Accenture under the Agreement. Client Data shall not include any component of the ACP Services or material provided by or on behalf of Accenture.
"**CMP Services**" has the meaning given to it in Section 2.2.2;
"**CMS Services**" has the meaning given to it in Section 2.2.3;
"**Confidential Information**" means information that relates to the other Party's (or to Cloud Vendor's) past, present, or future research, development, business activities, products, services, and technical knowledge, which is identified by the discloser as confidential or that would be understood to be confidential by a reasonable person under the circumstances. For the purposes of this Agreement, the term "Confidential Information" does not include Client Data;
"**Effective Date**" means the date first written above;
"**End User**" means any individual or entity that, directly or indirectly through another End User, accesses or uses the ACP Services, or accesses or uses the Client Data;
"**Fees**" means the fees specified in the relevant Service Order and payable in accordance with Section 6 or the relevant Service Order;
"**High Risk Activities**" means Usage such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems environments where the use or failure of the Service could lead to death, personal injury or environmental damage;
"**Infrastructure Services**" has the meaning given to it in Section 2.2.1;
"**Intellectual Property Rights**" means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights, derivatives thereof, and forms of protection of a similar nature; s
"**Service Order"** means the documents referenced in Section 1.2, and its exhibits, and any other documents incorporated by reference herein, together with any amendments thereto duly executed by the Parties;
"**Term**" has the meaning set forth in Section 11;
"**Termination Fees**" has the meaning set forth in the relevant Service Order;
"**Transformation Services**" has the meaning given to it in Section 2.2.4; and
"**Virus**" means any item, software, device or code which is intended by any person to, or which is likely to, or which may:

(a) impair the operation of any software or computer systems;
(b) cause loss of, or corruption or damage to any software or computer systems or data;
(c) prevent access to or allow unauthorised access to any software or computer system or data; and / or
(d) damage the reputation of the Client and / or Accenture,

including any computer virus, Trojan horse, worm, software bomb, authorization key, license control utility or software lock.

ACCENTURE INSIGHTS PLATFORM AGREEMENT

This **ACCENTURE INSIGHTS PLATFORM AGREEMENT ("AGREEMENT")** is made and entered into as of **[**Date**]**, ("**Effective Date**") by and between Accenture LLP, with offices at 161 N. Clark St. Chicago, IL 60601 ("**Accenture**") and *[Client]* ("**Client**"). Accenture and Client are also each referred to under this Agreement individually as a "**Party**," and together as the "**Parties**."

1 AGREEMENT STRUCTURE AND INTERPRETATION

1.1 This Agreement sets out the general terms and conditions for Accenture's provision of the Platform for Client's access and use, as further defined hereunder.

1.2 The specifics concerning the Platform to be provided by Accenture shall be detailed in a Service Order, to be executed by both Parties. Each executed Service Order constitutes a separate and binding agreement, incorporating the terms and conditions of this Agreement.

1.3 The capitalized terms as used in this Agreement have the meanings set out in the body of this Agreement or in **Exhibit A** (Definitions).

1.4 If there is a conflict between the terms and conditions of this Agreement and those of any Service Order, then the following order of precedence shall apply: (i) the Schedules to the Service Order and any other documents incorporated therein by reference; (ii) the Service Order; (iii) the terms and conditions of this Agreement; and (iv) any Exhibits to this Agreement.

2 CLIENT'S RIGHTS AND OBLIGATIONS

2.1 Subject to the terms and conditions of this Agreement and the relevant Service Order, Accenture hereby grants to Client a non-exclusive, non-transferable right during the term of the applicable Service Order to permit its Authorized Users to access and use the Platform and the Platform Outputs for authorized users' Permitted Purpose only.

2.2 Client acknowledges and agrees that it is solely responsible for (i) determining the suitability of the Platform for its purposes and those of its Authorized Users, and (ii) ensuring that the way that it and its Authorized Users access and use the Platform complies with any applicable laws.

2.3 Client agrees that it shall not license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit the Platform by making it or any portion of it available for access or use by any third party (except Authorized Users), including by means of operating a service bureau, outsourcing or time-sharing service.

2.4 Client shall be solely responsible for ensuring that Client's or its Authorized Users' use of the Platform Services shall not exceed any restrictions contained in the applicable Service Order. *[In particular, the Client shall ensure that (i) if applicable, the maximum number of Authorized Users that it authorises to access and use the Platform Services shall not exceed the number of user subscriptions it has purchased from time to time as set out in a Service Order, and (ii) it will not allow or suffer any user account to be used by more than one individual Authorized User unless it has been reassigned in its entirety to another individual Authorized User, in which case the prior Authorized User shall no longer have any right to access or use the Platform Services.]*

2.5 Client is responsible for all use of the Platform by those who have access to it through Client's credentials, and for ensuring that its Authorized Users do not circumvent or disclose any usernames, passwords or other access credentials or authentication details, or interfere with or disrupt any other security control of the Platform.

2.6 Client shall maintain commercially reasonable security standards for its and its Authorized Users' use of the Platform. Specifically, Client will use good industry practice virus protection software, and other customary procedures to screen any Client Content to avoid introducing any Virus or other malicious files or other harmful code that could disrupt the proper operation of the systems used in the provision of the Platform. Client also agrees that it shall use all reasonable endeavors to ensure that its Authorized Users do not upload or distribute files that contain Viruses, or do anything else to disrupt or attempt to disrupt, the systems and networks used for the provision of the Platform. If Client learns or suspects that its Authorized Users have introduced a Virus, Client will notify Accenture and cooperate in mitigating the effects of such Virus and, in the event a Virus or other such code is introduced into the systems used to deliver the Platform due to Client's failure to use such endeavours, Client will at its cost assist Accenture in mitigating the effects.

2.7 Client shall be solely responsible for the acts and omissions of its Authorized Users as if they were the acts and omissions of Client, and for ensuring that anyone who uses the Platform does so in accordance with the terms and conditions of this Agreement and the applicable Service Order. In particular, the Client agrees that it shall not, and that it shall ensure that its Authorized Users do not: (i) access or use the Platform to host or transmit any content, data or information that is illegal or which infringes any third party's rights, such as intellectual property rights or right of privacy, or which otherwise violates any applicable laws; (ii) copy, translate, make derivative works, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code or underlying ideas or algorithms embodied in the software applications or other systems used for the provision of the Platform, unless expressly permitted under any applicable laws, or remove any titles or trademarks, copyrights or restricted rights notices in the systems, software and other materials used in the provision of the Platform; (iii) distribute, sell, sublicense, rent, lease or use the Platform (or any portion thereof) for time sharing, hosting, service provider or like purposes; (iv) remove any product identification, proprietary, copyright or other notices contained in the Platform; (v) utilize any equipment, device, software, or other means designed to circumvent or remove any form of product key or copy protection used by Accenture or its vendors or use the Platform together

with any authorization code, product key, serial number, or other copy protection device not supplied by Accenture or its vendors; (vi) use the Platform to access a database outside of the Platform; (vii) access or use the Platform to develop a product that is competitive with the Platform or a software application within the Platform; (viii) make any benchmarking results for any such software application available to any third parties; (ix) access or use the Platform in a way intended to avoid incurring fees or exceeding usage limits or quotas; (x) access or use the Platform in a way that poses a security risk to or may otherwise adversely impact the Platform; (xi) access or use the Platform in a way that infringes or otherwise violates the rights or other interests of a third party, entails illegal or otherwise prohibited content or activities, or otherwise subjects Accenture or its licensors to a potential liability.

2.8 Client will notify Accenture immediately it becomes aware of any breach or threatened breach of the terms of this Section 2, or of any breach or threatened breach of security including any attempt by a third party to gain unauthorized access to the systems used for the provision of the Platform.

2.9 Client acknowledges and agrees that it is responsible for obtaining and maintaining its own hardware, software, communications equipment and network connections necessary to access the Platform, and for paying any applicable third-party fees and charges incurred while accessing and using the Platform Services. To the extent that the Software includes any open source components and those components are subject to an open source license which is delivered with the Software, then the terms of that open source license shall apply and prevail to the extent of any conflict, but only insofar as they relate to such open source components and not to any other part of the Software. Licensee shall comply with the terms of such open source license.

3 **ACCENTURE'S RIGHTS AND OBLIGATIONS**

3.1 Accenture shall make available and support the Platform in accordance with an executed Service Order.

3.2 If the Parties so agree in any applicable Service Order, Accenture may also provide certain additional services (such as systems integration, professional, and/or management consulting services, etc.) in connection with the Platform ("**Additional Services**"), in which case the terms in the Service Order applicable to Additional Services shall apply.

3.3 Accenture will use accepted industry standard security technologies (e.g. encryption, password protection and firewall protection) in providing the Platform.

3.4 Accenture may need to apply updates or make changes to the Platform that it is providing pursuant to any Service Order, provided always that Accenture shall not be entitled to apply such updates or other changes in a manner that would make the Platform non-conforming with the applicable service descriptions, or otherwise materially diminish the scope or the quality of the service provided, unless such changes are necessary for Accenture to comply with any applicable laws. Accenture will notify the Client reasonably in advance of any planned changes to the Platform Services that have any material impact on Client's access to or use of the relevant service.

3.5 Client acknowledges and agrees that Accenture shall be permitted to monitor the Client's and its Authorized Users' access and usage of the Platform limited solely for the purposes of verifying Client's compliance with the terms of this Agreement and the applicable Service Order.

3.6 Client hereby acknowledges, accepts and agrees that Accenture may have to suspend Client's and/or its Authorized Users' right to access or use all or any portion of the Platform, or remove any relevant Client Content as described below, (i) where such access or use, or any Client Content is in breach of Section 2.7; (ii) where Client fails to pay to Accenture any amounts due within thirty (30) days of such payments being due; or (iii) where Accenture is required to do so under any applicable laws, or any court's or governmental body's order.

3.7 When allowed under the applicable laws and if otherwise reasonable under the circumstances (as determined by Accenture in its discretion), Accenture shall provide Client with a written notice prior to such suspension, and an opportunity to take steps to avoid any such suspension. Any suspension of Client's or its Authorized Users' right to access or use the Platform shall not release the Client from its obligations under this Agreement and any Service Order, including any obligation of paying the fees. Accenture's suspension right is in addition to Accenture's right to terminate this Agreement or any Service Order pursuant to Section 10.

4 **CLIENT CONTENT**

4.1 Client (and Client's licensors, where applicable) own all right, title and interest in and to the Client Content.

4.2 Client acknowledges and agrees that it is solely responsible for complying with any regulations, laws, or conventions applicable to the Client Content. In particular, Client agrees that it has collected and shall maintain and handle all Regulated Information contained in Client Content in compliance with all applicable data privacy and protection laws, rules and regulations. *[Client authorizes*

Accenture to process its Regulated Information in accordance with the applicable data protection laws and regulations, and any data processing provisions incorporated in or referred to in the applicable Service Order.] OR

4.3 *[In this Section **process**, **processor**, **controller**, **data subject** and **personal data** shall have the meaning given in the EU Directive 95/46/EC. Client hereby appoints Accenture as processor in relation to personal data (i) which Accenture receives under or in connection with the performance of the Platform; and (ii) in respect of which Client is a controller.*

4.4 *In processing any personal data pursuant to this Agreement or any Service Order, Accenture shall (i) act only on written instructions from Client; and (ii) unless otherwise requested by Client, process personal data only to the extent, and in such manner, as is necessary for the provision of the Platform.*

4.5 *In appointing Accenture as a processor under this Agreement or a Service Order, Client has satisfied itself that Accenture and any applicable Cloud Vendor have in place appropriate technical and organizational measures to protect the personal data processed on behalf of Client from unauthorized use or access, accidental loss, damage, destruction, theft or disclosure.]*

4.6 Client shall have the ability to access its Client Content hosted in the Platform Services at any time during the Term set forth in the applicable Service Order. Client may export and retrieve its Client Content during the said Term, subject to any technical limitations in the Platform Services or Client hardware and software (and that of its Authorized Users), including factors such as (i) the size of Client's instance of the Platform Services; and (ii) the frequency and/or timing of the export and retrieval.

4.7 Client acknowledges and agrees that Accenture does not control the transfer of data over the internet or a public telecommunications network and that accordingly the Accenture's obligations set forth in this Agreement and in the Service Order shall not apply to Client Content that is transmitted by or on behalf of Client or its Authorized Users over such networks.

4.8 Client grants to Accenture the nonexclusive right to host, store, process, modify, and transfer the Client Content for the purposes of Client's use of the Platform as provided in this Agreement and Accenture's improvement or enhancement of the Platform incidental to such use. Upon expiration or termination of the Agreement, Accenture agrees to destroy any Client Content in accordance with this Agreement.

5 FEES, PAYMENTS AND TAXES

5.1 Client shall pay the fees specified in the applicable Service Order. Fees are stated exclusive of all applicable duties, tariffs, and taxes. Unless otherwise specified in a Service Order, fees will be due and payable within thirty (30) days of Accenture's invoice. Late payments that are not the subject of a good faith dispute are subject to an interest charge, which is the lesser of: (a) one and one-half percent (1.5%) per month, or (b) the maximum legal rate.

5.2 Client will provide any information reasonably requested by Accenture to determine whether Accenture is obligated to collect VAT and sales tax from Client, including Client's VAT and sales tax identification number. If Client is legally entitled to an exemption from any sales, use, or similar transaction tax, Client is responsible for providing Accenture with legally-sufficient tax exemption certificates for each taxing jurisdiction. Accenture will apply the tax exemption certificates to charges under Client's accounts occurring after the date Accenture receives the tax exemption certificates. If any deduction or withholding is required by applicable law, Client will notify Accenture and will pay any additional amounts necessary to ensure that the net amount that Accenture receives, after any deduction and withholding, equals the amount Accenture would have received if no deduction or withholding had been required. Additionally, Client will provide Accenture with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

5.3 Client will be responsible for the payment of all taxes in connection with this Agreement including, but not limited to, sales, use, excise, value-added, business, service, goods and services, consumption, withholding, and other similar taxes or duties, including taxes incurred on transactions between and among Accenture, its Affiliates, and third party subcontractors. Client will reimburse Accenture for any deficiency relating to taxes that are Client's responsibility under this Agreement. Each Party will be responsible for its own income taxes, employment taxes, and property taxes. The Parties will cooperate in good faith to minimize taxes to the extent legally permissible. Each Party will provide to the other Party any resale exemption, multiple points of use certificates, treaty certification and other exemption information reasonably requested by the other Party.

5.4 All amounts payable under this Agreement will be made without set-off or counterclaim, and without any deduction or withholding.

6 ACCENTURE'S INTELLECTUAL PROPERTY RIGHTS

6.1 Accenture (and its licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to the systems, software and other content and materials used in the provision of the Platform. In addition, Client agrees that Accenture (and its licensors, where applicable) will own all right, title and interest in and to any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Client or any other Party relating to the Platform, and Client hereby assigns any intellectual property rights in such items to Accenture. The Accenture name, the Accenture logo, and the product names associated with the Platform are trademarks of Accenture or third parties, and no right or license is granted to Client to use them.

7 WARRANTIES AND EXCLUSIONS

7.1 Accenture warrants that the Platform provided to Client pursuant to this Agreement will comply in all material respects with the applicable Service Order. This warranty shall not apply where: (i) the Client's or any Authorized User's access to or use of the Platform

is not in accordance with this Agreement, the relevant Service Order (or any Exhibits to the relevant Service Order) or with Accenture's instructions; (ii) modification or alteration of the Platform or any systems, software or other content or materials embodied therein is made by any Party other than Accenture; or (iii) the Platform is being provided free of charge, or as a trial, pre-release or as a beta release.

7.2 Client shall provide Accenture with prompt written notice of any non-conformity of the Platform, sufficiently describing such non-conformity, no later than within thirty (30) days of the appearance or Client's discovery of such non-conformity.

7.3 In such event, Accenture will use commercially reasonable efforts to correct any such non-conformity. In the event Accenture is unable to correct such non-conformity by exercising commercially reasonable efforts for a reasonable period of time, either Party may terminate the relevant Service Order concerning the non-conforming Platform Service(s) on written notice to the other Party in which case as Client's sole and exclusive remedy, Accenture will provide a pro-rated refund of any pre-paid Fees for periods after the effective date of termination.

7.4 **Disclaimer.** EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 7, ACCENTURE, ITS AFFILIATES AND ITS LICENSORS MAKE NO REPRESENTATIONS AND PROVIDE NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE PLATFORM OR ANY THIRD PARTY COMPONENTS OR CONTENT EMBODIED THEREIN, INCLUDING ANY WARRANTY THAT ACCESS TO AND USE OF THE PLATFORM WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING CLIENT CONTENT OR THIRD PARTY COMPONENTS OR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED, AND 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. EACH PARTY, ITS AFFILIATES AND ITS LICENSORS DISCLAIM ALL, AND THE OTHER PARTY AGREES THAT IT IS NOT ENTITLED TO ANY EQUITABLE OR IMPLIED INDEMNITIES. THESE DISCLAIMERS SHALL ONLY APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW.

7.5 **High Risk Activities.** Accenture, on behalf of itself and its Affiliates and licensors and the Cloud Vendor, specifically disclaims any express or implied warranty of fitness of the Platform for High Risk Activities.

8 **THIRD PARTY CLAIMS**

8.1 Subject to the limitations in Section 9, Accenture will defend (at its sole expense) Client and Client's Affiliates against any claims brought against Client by any third party (that is not an Affiliate of Client) alleging that Client's use of the Platform, in accordance with the terms and conditions of the Agreement and the applicable Service Order, constitutes a direct infringement of a patent issued in the United States as of the Effective Date, copyright, or trade secret of any third party . Accenture will only be obliged to pay the amount of any damages finally awarded against Client or the amount of any settlement agreed by Accenture.

8.2 Accenture will have no obligations or liability under Section 8.1 for any claims to the extent arising from:

8.2.1 Client Content;

8.2.2 Client's or any Authorized User's use of the Platform after Accenture has notified Client, in accordance with this Agreement, to discontinue such use and Client have been afforded a reasonable opportunity to discontinue such use;

8.2.3 any unauthorized modification or unauthorized use of the Platform where infringement or misappropriation would not have occurred but for such unauthorized modification or unauthorized use;

8.2.4 any use of the Platform, or any other act, by Client or an Authorized User, that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for the breach;

8.2.5 [*any claim of wilful infringement adjudicated against anyone other than Accenture and its Affiliates or Cloud Vendor;*]

8.2.6 any combination(s) of the Platform with any other product, service, software, content, data or method not supplied by Accenture; or

8.2.7 a free (no fee) or trial license of the Platform.

8.3 If any portion of the Platform is alleged to infringe any third party Intellectual Property Rights, Accenture may choose (at its election and expense) to: (a) procure the rights to use the item alleged to be infringing; (b) replace the alleged infringing portion with a non-infringing equivalent; or (c) modify the alleged infringing portion to make it non-infringing while still providing substantially the same level of functionality. If Accenture determines the actions from Section 8.3 (a) to (c) are not commercially reasonable, Accenture may immediately terminate Client's access to the Platform.

8.4 Client shall warrant that (i) any use of Platform by Client or its Authorized Users will not be in violation of any applicable law or regulation; or (ii) Client will not place content that violates, infringes or misappropriates the rights of a third party; (iii) Client's or its Authorized Users' use of the Platform or other act will not be in violation of this Agreement or the relevant Service Order; (iv) Client will not place infringing materials on the Platform; (v) Client's data hosted on the Platform is owned and/or licensed for use in such

an environment as the Platform; (vi) Client has the necessary licenses to possess its data hosted on the Platform; and (vii) Clients or any Authorized Users will not engage in High Risk Activities.

8.5 Client will have no warranty obligations where:

8.6.1 Client has notified Accenture, in accordance with the terms of this Agreement, to delete the Client Content from the SaaS and Accenture has been afforded a reasonable opportunity to do so; or

8.6.2 any unauthorized access or use of the Client Content by Accenture that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for such breach.

8.6 [reserved]

8.7 **Exclusive Remedy**. SECTION 8.1 CONSTITUTES CLIENT'S SOLE AND EXCLUSIVE REMEDY AND ACCENTURE'S (AND ITS AFFILIATES') ENTIRE OBLIGATION TO CLIENT WITH RESPECT TO ANY CLAIM THAT THE PLATFORM INFRINGES OR MISAPPROPRIATES THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

9 **LIMITATION OF LIABILITY**

9.1 EXCEPT FOR *[(I) THE PARTIES' OBLIGATIONS UNDER SECTION 8;*] (II) DAMAGES RESULTING FROM A BREACH OF A PARTY'S OBLIGATIONS IN SECTION 11 WITH RESPECT TO CONFIDENTIAL INFORMATION; (III) DAMAGES RESULTING FROM DEATH OR BODILY INJURY ARISING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OR FROM FRAUD OR FRAUDULENT MISREPRESENTATION; AND (IV) ACCENTURE'S RIGHT TO COLLECT UNPAID FEES DUE HEREUNDER, UNDER NO CIRCUMSTANCES AND REGARDLESS OF THE NATURE OF ANY CLAIM SHALL EITHER PARTY (OR THEIR RESPECTIVE AFFILIATES OR ACCENTURE'S LICENSORS) BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY UNDER THE AGREEMENT FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID FOR THE APPLICABLE PLATFORM SERVICE IN THE TWELVE (12) MONTH PERIOD PRECEDING THE DATE OF THE INCIDENT GIVING RISE TO LIABILITY.

9.2 TO THE EXTENT PERMITTED BY LAW NEITHER PARTY NOR ANY OF EITHER PARTY'S RESPECTIVE AFFILIATES WILL BE LIABLE TO THE OTHER PARTY UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES; BUSINESS INTERRUPTION, LOSS OF PROFITS OR SAVINGS, REVENUES, OR GOODWILL; LOSS OR CORRUPTION OF DATA; UNAVAILABILITY OF ANY OR ALL OF THE PLATFORM; INVESTMENTS, EXPENDITURES OR COMMITMENTS RELATED TO USE OF OR ACCESS TO THE PLATFORM; COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; UNAUTHORIZED ACCESS TO, COMPROMISE, ALTERATION OR LOSS OF CLIENT CONTENT OR BUSINESS INFORMATION; OR COST OF REPLACEMENT OR RESTORATION OF ANY LOST OR ALTERED CLIENT CONTENT.

9.3 Notwithstanding anything in this agreement to the contrary, the foregoing limitations on liability shall apply to any damages arising out of a Security Breach. The Parties acknowledge that the limitations on liability set out in this Section 9 are essential terms of this Agreement and the Parties would not have entered this Agreement without them.

9.4 No action, regardless of form, arising out of this Agreement may be brought by Client more than two (2) years after Client knew or should have known of the event which gave rise to the cause of action.

10 **TERM AND TERMINATION**

10.1 The term of this Agreement will commence on the Effective Date and will continue until terminated by either Party pursuant to this Section 10 ("**Term**"). The term of any Service Order shall be agreed in the Service Order itself, and the terms and conditions of this Agreement shall survive and remain in force to govern any Service Order the term of which exceeds any termination of this Agreement.

10.2 Either Party may terminate this Agreement (but not a Service Order) for convenience upon [sixty (60) days] written notice to the other Party. For the avoidance of doubt, either Party may only terminate a Service Order in accordance with the terms of the Service Order or as expressly provided for in this Agreement.

10.3 Either Party may terminate this Agreement and/or any Service Order upon written notice if the other Party ceases its business operations or becomes subject to insolvency proceedings or any similar or equivalent process in any jurisdiction, and the proceedings are not dismissed within ninety (90) days, or otherwise becomes generally unable to meet its obligations under this Agreement and/or the Service Order.

10.4 In addition to any other remedies that a Party may have at Law, in equity, or under this Agreement, a Party may terminate this Agreement and/or any Service Order upon [thirty(30)] days' advance written notice to the other Party if the other Party commits any material breach of this Agreement and/or any Service Order and fails to cure such default (if curable) within the [thirty (30)] day period, including if there has been any such act or omission by Client or any Authorized User that has given Accenture the right to suspend the provision of Platform in accordance with Section 3.6.

10.5 Accenture may also terminate this Agreement and/or any Service Order without liability upon [thirty (30)] days' notice to Client or any Authorized User: (i) in the event where an underlying contract between Accenture and the Cloud Vendor concerning the hosting

of AIP terminates, or (ii) if termination of the Agreement and/or any Service Order is necessary to comply with applicable law or binding requests of governmental entities.

10.6 Upon the effective date of expiration or termination of a Service Order, Accenture shall immediately cease Client's and its Authorized Users' access to and use of the Platform

10.7 Where so agreed in the applicable Service Order, Accenture will provide Client with the ability to retrieve Client Content after the expiry or termination of the said Service Order for a limited period of time, in which instance the Client will cover the costs of the data storage unless otherwise agreed in the Service Order. Otherwise, Accenture may destroy (or procure the destruction of) or otherwise dispose of any Client Content in its possession or that of a Cloud Vendor (including any data back-ups) upon expiry or termination of the applicable Service Order.

10.8 If so mutually agreed in the Service Order, Accenture shall provide to Client reasonable co-operation and assistance to facilitate the orderly wind down of the usage of the Platform and/or to assist Client to transition to another provider. Client will pay Accenture for such assistance at Accenture's then-current time and materials rates for the applicable services or as otherwise mutually agreed by Client and Accenture. If the termination results from a breach of this Agreement by Client, Accenture may invoice Client in advance for all transition assistance services and, if so invoiced, Client will pay in advance.

11 **CONFIDENTIALITY**

11.1 Each Party agrees that it will use the other Party's Confidential Information only to the extent reasonably necessary for purposes of this Agreement or a Service Order. Each Party agrees to take reasonable steps to protect the other's Confidential Information, provided that these steps must be at least as protective as those the Party takes to protect its own Confidential Information of similar nature, but in any event no less than a reasonable standard of care.

11.2 Each Party may disclose the other Party's Confidential Information to its Affiliates, employees, contractors, licensors and agents who: (a) have a need to know it for purposes contemplated by this Agreement, and (b) are legally bound to protect the Confidential Information on terms no less protective than the terms of this Agreement.

11.3 This Section 11 will not apply to any information that either Party can demonstrate: (a) was at the time of disclosure or that has become thereafter published or otherwise becomes publicly available at no fault of the receiving Party; (c) was in the possession of the receiving Party at the time of disclosure to it and was not the subject of a pre-existing confidentiality obligation; (d) was received after disclosure to it from a third party who had a lawful right to disclose such information (without corresponding confidentiality obligations) to it; or (e) was independently developed by the receiving Party without use of the Confidential Information of the disclosing Party.

11.4 The receiving Party will not be considered to have breached its obligations under this Section 11 for disclosing Confidential Information of the disclosing Party to the extent required to satisfy any legal requirement of a competent governmental or regulatory authority, provided that promptly upon receiving any such request and to the extent that it may legally do so, the receiving Party: (i) advises the disclosing Party prior to making such disclosure in order that the disclosing Party may object to such disclosure or take any other action that it considers appropriate to protect the Confidential Information and; (ii) takes actions necessary to minimize any disclosure to only that necessary to satisfy any legal requirement of a competent governmental or regulatory authority (including through redaction of sensitive commercial information, where legally permissible).

11.5 Any reproduction of any Confidential Information of the other Party shall remain the property of the disclosing Party, and the disclosing Party may, at any time including on termination or expiration of this Agreement, request the receiving Party to return, destroy or delete (and confirm the destruction or deletion of the same) as instructed (in such a manner that it cannot be recovered) all Confidential Information of the disclosing Party in the receiving Party's possession or control. Notwithstanding the foregoing, each Party may archive all copies of Confidential Information that it is required to retain to comply with law and its other record-keeping requirements.

11.6 Client shall not disclose the terms and conditions of this Agreement or the pricing contained herein to any third party unless otherwise agreed by the Parties. Neither Party will use the name of the other Party without the prior written consent of the other, except that Client agrees that Accenture may use Client's name in customer listings or quarterly calls with its investors or, at times mutually agreeable to the parties, as part of Client's marketing efforts (including reference calls and stories, press testimonials, and prospective customer meetings).

12 **ADDITIONAL TERMS**

12.1 **Compliance with Laws.** Accenture will comply with all Laws applicable to it in providing Client with access to the Platform and Client will comply with all Laws applicable to it and its business in providing the Client Content and in using the Platform and the Platform Outputs. Each Party will comply with all export control and economic sanctions laws applicable to its performance under this Agreement. Client agrees that Client will and will procure that Authorized Users do not use the Platform in or in relation to any activities involving a country subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria or the Crimea region of Ukraine), or involving a Party in violation of such applicable trade control laws, or that require government authorization, without first obtaining the informed consent of Accenture and the required authorization. For the avoidance of doubt, Client shall not grant access to the Platform to any individual, entity or organization which is subject to trade

sanctions or embargos by the United States or any applicable jurisdiction, including any individual, entity or organization which is listed on the OFAC Specially Designated Nationals List from time to time.

12.2 **Notices**. Unless expressly stated otherwise in this Agreement, all notices under this Agreement must be in writing and must be delivered personally, sent by certified mail (return receipt requested); or sent by express courier (with confirmation of delivery). The notice will be deemed given and will be effective upon receipt: (a) when it is delivered to a Party personally; (b) upon receipt if sent certified mail, return receipt requested; or (c) when delivered by a nationally recognized overnight courier service such as FedEx (with confirmation of delivery). Any notice by email will only be allowed in the particular Sections of this Agreement that expressly permit it. All notices must be addressed to the other Party at the address set forth in the preamble above. Either Party may designate a different address by giving ten (10) days' written notice to the other Party in accordance with this Agreement. A copy of any notice under the terms of this Agreement (except for invoices and other routine correspondence) will be forwarded to: Accenture LLP, Legal – General Counsel, 161 North Clark Street, Chicago, Illinois 60601. Such copy will not constitute effective notice. All communications and notices to be made or given pursuant to this Agreement must be in the English language.

12.3 **Governing Law and Jurisdiction**. The laws of [the State of Illinois and federal laws of the United States] will govern the construction, validity and operation of this Agreement and the performance of all obligations hereunder without regard for Illinois' choice of law provisions. The courts of [Chicago, Illinois] shall have exclusive jurisdiction in relation to any dispute or matter arising under or in connection with this Agreement.

12.4 **Force Majeure**. Other than Client's obligation to pay Accenture pursuant to this Agreement and any Service Order, neither Party will be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond its reasonable control, including but not limited to electrical or power outage, utilities or telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war, or labour disputes with its or its affiliates' employees, industrial disturbances.

12.5 **Survival**. The provisions of Sections 6, 7.4, 8, 9, 11 and 12, and any other Sections which by their nature are intended to survive, will survive the termination or expiration of this Agreement.

12.6 **Assignment**. Client may not assign this Agreement or delegate or sublicense any of Client's rights or obligations hereunder, including by operation of law, without the prior written consent of Accenture and any attempt to do so in violation of this provision will be null and *void*. This Agreement will be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns.

12.7 **Variation**. Except as otherwise expressly provided to the contrary in this Agreement, this Agreement may only be changed, modified or expanded by a writing signed by both Parties.

12.8 **No waiver**. No delay, neglect or forbearance on the part of either Party in enforcing against the other any term or condition of this Agreement will be deemed to be a waiver nor will it in any way prejudice any right of that Party under this Agreement nor will any single or partial exercise of any right preclude any other or further exercise of these rights or any other right.

12.9 **Severability**. The invalidity or unenforceability of any provision of this Agreement will not affect the validity or enforceability of any other provision hereof and it is the intent and agreement of the Parties that this Agreement will be deemed amended by modifying such provision to the extent necessary to render it valid, legal and enforceable while preserving its intent or, if such modification is not possible, by substituting another provision that is legal and enforceable and that achieves the same objective. The Parties agree that any principle of construction or rule of law that provides that an agreement will be construed against the drafter will not apply to this Agreement.

12.10 **Entire Agreement**. This Agreement, along with any Service Orders, attachments, exhibits, Attachments or referenced documents or agreements attached hereto from time to time, contains the entire Agreement between the Parties with respect to the matters specified herein and supersedes all prior or contemporaneous representations, understandings, agreements or communications between Accenture and Client, whether written or verbal, regarding the subject matter of this Agreement.

12.11 **Relationship of the Parties**. Nothing in this Agreement will be deemed to create a joint venture, partnership, or agency relationship between the Parties or be deemed to authorize either Party to incur any liabilities or obligations on behalf of, or in the name of, the other.

12.12 **Third Party Rights**. Accenture's licensors are third party beneficiaries hereunder. This Agreement does not otherwise create any third party beneficiary rights, and in particular it is agreed that Client's Authorized Users are not third party beneficiaries. Accenture and Client are independent contractors.

12.13 **Existing Agreements**. This Agreement is separate from any obligations, rights, or requirements contained in any existing master services agreement, professional services agreement, consulting services agreement, outsourcing agreement, or related agreements ("**Existing Agreements**") between the Parties. Any Existing Agreement will not apply to the products and services that are the subject of this Agreement, and this Agreement expressly overrides any conflicting statements in any Existing Agreement.

12.14 **Counterparts.** This Agreement may be executed in any number of counterparts and executed by facsimile or by other electronic communication as agreed upon by the Parties, such execution to be considered an original for all purposes, and all of which together will constitute one and the same instrument, notwithstanding that the Parties may not both be signatories to the original or same counterpart.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly Authorized representatives and caused it to be effective as of the date first written above.

ACCENTURE:	**Client: ARIZONA DEPARTMENT OF ADMINISTRATION _____**
BY:_____	BY:_____
PRINTED NAME: _____	PRINTED NAME: _____
TITLE: _____	TITLE: _____
DATE:_____	DATE: _____

EXHIBIT A

Definitions

"**Additional Services**" has the meaning given to it in Section 2;
"**Affiliate**" of a Party means any entity, whether incorporated or not, that is Controlled by, Controls, or is under common Control with such Party. "Control" means the ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise;
"**Agreement**" means this Accenture Platform Agreement, any exhibits attached hereto and any other documents incorporated hereto by reference, together with any amendments hereto duly executed by the Parties;
"**Authorized User**" means any individual or entity that, directly or indirectly through another Authorized User, accesses or uses the Platform;
"**Cloud Vendor**" means the cloud service provider that is hosting AIP;
"**Client Content**" means any content, materials, data and information, *[including Regulated Information] OR [personal data (as defined in Section 4.3]*, that is introduced to the Platform by or on behalf of Client or its Authorized Users. Client Content shall not include any component of the Platform or material provided by or on behalf of Accenture.
"**Confidential Information**" means information that relates to the other Party's (or to Cloud Vendor's) past, present, or future research, development, business activities, products, services, and technical knowledge, which is identified by the discloser as confidential or that would be understood to be confidential by a reasonable person under the circumstances;
"**Effective Date**" means the date first written above;
"**Fees**" means the fees specified in the relevant Service Order and payable in accordance with Section 6 or the relevant Service Order;
"**High Risk Activities**" means usage such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems environments where the use or failure of the Service could lead to death, personal injury or environmental damage;

"**Intellectual Property Rights**" means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights and forms of protection of a similar nature, including to any derivative works, enhancements or modifications;
"Permitted Purpose" means Client's internal business purposes;
"**Law" or "Laws"** means all applicable local, state, national, and international laws, treaties and regulations, codes, ordinances, rules, restrictions, licenses, and judicial or administrative orders that are in effect at the time;
"**Platform Outputs**" or **"Outputs"** means the downloadable files consisting of visualizations, charts, graphs, reports or other data displayed or produced via the Platform, but excluding models, software, and Client Data
"**Platform"** means the Accenture Insights Platform, also known as AIP, a hosted solution made available by Accenture for access and use on a subscription basis, as detailed in the applicable Service Order. The Platform includes any modifications, enhancements, additions, extensions, translations and derivative works thereof and any configuration and related services. Platform does not include Client Content or any Client-provided third party software;
"**Regulated Information**" means: (a) data which names or identifies a natural person; (b) data that is explicitly defined as a regulated category of data under data privacy laws applicable to Client; (b) non-public personal data, such as national identification number, passport number, social security number, driver's license number; (d) health or medical information, such as insurance information, medical prognosis, diagnosis information or genetic information; (e) financial information; and/or (f) sensitive personal data, such as race, religion, marital status, disability, or sexuality;
"**Security Breach**" means a failure by Accenture to comply with the Security Standards, where such failure results in the unauthorized access to or acquisition of any unencrypted record in Accenture's control containing Client Content in a manner that renders misuse of the Client Content reasonably possible. For the avoidance of doubt, Security Breach does not include any of the following that results in no unauthorized access to Client Content or to any Accenture or Cloud Vendor systems storing Client Content: (a) pings and other broadcast attacks on firewalls or edge servers, (b) port scans, (c) unsuccessful log-on attempts, (d) denial of service attacks, (e) packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers), or (f) similar incidents.;
"**Security Standards**" means the AIP security standards, as defined in the Service Order.
"**Service Order"** means the documents referenced in Section 1.2, and its Schedules, and any other documents incorporated by reference herein, together with any amendments thereto duly executed by the Parties;
"**Service Order Term**" means the term applicable to the Service Order as set forth in Schedule 1 thereto.
"**Term**" has the meaning set forth in Section 10;
"**Virus**" means any item, software, device or code which is intended by any person to, or which is likely to, or which may:

(a) impair the operation of any software or computer systems;
(b) cause loss of, or corruption or damage to any software or computer systems or data;
(c) prevent access to or allow unauthorised access to any software or computer system or data; and / or
(d) damage the reputation of the Client and / or Accenture,

including any computer virus, Trojan horse, worm, software bomb, authorization key, license control utility or software lock.

ACCENTURE VIRTUAL ASSISTANT PLATFORM AGREEMENT

This **ACCENTURE VIRTUAL ASSISTANT PLATFORM AGREEMENT ("AGREEMENT")** is made and entered into as of **[**INSERT DATE**]**, ("**Effective Date**") by and between [INSERT APPROPRIATE ACCENTURE ENTITY**]**, with offices at [INSERT REGISTERED ACCENTURE ADDRESS] ("**Accenture**") and [INSERT CLIENT NAME] with offices at [INSERT REGISTERED CLIENT ADDRESS] ("**Client**"). Accenture and Client are also each referred to under this Agreement individually as a "**Party**," and together as the "**Parties**."

1 **AGREEMENT STRUCTURE AND INTERPRETATION**

1.1 This Agreement sets out the general terms and conditions for the provision of the Platform Services by Accenture to Client, as further defined hereunder.

1.2 The specifics concerning the Platform Services to be provided by Accenture shall be detailed in a Service Order, to be executed by both Parties. Each executed Service Order constitutes a separate and binding agreement, incorporating the terms and conditions of this Agreement.

1.3 The capitalized terms as used in this Agreement have the meanings set out in the body of this Agreement, **Exhibit A** (Definitions) or the applicable Service Order.

1.4 If there is a conflict between the terms and conditions of this Agreement and those of any Service Order, then the following order of precedence shall apply: (i) the Service Order; (ii) any Schedules to the Service Order and any other documents incorporated thereto by reference; (iii) the terms and conditions of this Agreement; and (iv) any Exhibits to this Agreement.

2 **CLIENT'S RIGHTS AND OBLIGATIONS**

2.1 Subject to the terms and conditions of this Agreement and the relevant Service Order, Accenture hereby grants to Client a non-exclusive, non-transferable right during the term of the applicable Service Order to permit its Authorized Users to access and use the Platform Services for the Permitted Purpose only.

2.2 Client acknowledges and agrees that it is solely responsible for (i) determining the suitability of the Platform Services for its purposes and those of its Authorized Users, and (ii) ensuring that the way that it and its Authorized Users access and use the Platform Services complies with any applicable laws. Client shall evaluate whether the design characteristics of the Platform Service to be provided by Accenture meet Client's regulatory requirements including any data privacy laws applicable to Client's business and use of the Platform Service. Client may propose any modifications to the Platform Services that Client believes are necessary in order for it to meet such requirements and any such modifications will be mutually agreed upon in writing in the Service Order or an amendment thereto. Any such use of the Platform Services by Client will be deemed acceptance and validation that the design characteristics meet Client's requirements.

2.3 Client agrees that, unless explicitly authorised pursuant to the Permitted Purpose, it shall not license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit the Platform Services by making them available for access or use by any third party (except Authorized Users), including by means of operating a service bureau, outsourcing or time-sharing service.

2.4 Client shall be solely responsible for ensuring that Client's or its Authorized Users' use of the Platform Services shall not exceed any restrictions contained in the applicable Service Order. In particular, the Client shall ensure that (i) if applicable, the maximum number of Authorized Users that it authorises to access and use the Platform Services shall not exceed the number of user subscriptions it has purchased from time to time as set out in a Service Order, and (ii) it will not allow or suffer any user account to be used by more than one individual Authorized User unless it has been reassigned in its entirety to another individual Authorized User, in which case the prior Authorized User shall no longer have any right to access or use the Platform Services.

2.5 Client is responsible for all use of the Platform Services by those who have access to them through Client's credential, and for ensuring that its Authorized Users do not circumvent or disclose any usernames, passwords or other access credentials or authentication details, or interfere with or disrupt any other security control of the Platform Services.

2.6 Client shall maintain commercially reasonable security standards for its and its Authorized Users' use of the Platform Services. Specifically, Client will use good industry practice regarding virus protection software, and other customary procedures to screen any Client Content to avoid introducing any Virus or other malicious files or other harmful code that could disrupt the proper operation of the systems used in the provision of the Platform Services. Client also agrees that it shall use all reasonable endeavors to ensure that its Authorized Users do not upload or distribute files that contain Viruses, or do anything else to disrupt or attempt to disrupt, the systems and networks used for the provision of the Platform Services.

2.7 Client shall be solely responsible for the acts and omissions of its Authorized Users as if they were the acts and omissions of Client, and for ensuring that anyone who uses the Platform Services does so in accordance with the terms and conditions of this Agreement and the applicable Service Order. In particular, the Client agrees that it shall not, and that it shall ensure that its Authorized Users do not: (i) access or use the Platform Services to host or transmit any content, data or information that is illegal or which infringes any third party's rights, such as intellectual property rights or right of privacy, or which

otherwise violates any applicable laws; (ii) copy, translate, make derivative works, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code or underlying ideas or algorithms embodied in the software applications or other systems used for the provision of the Platform Services (including the IaaS), unless expressly permitted under any applicable laws, or remove any titles or trademarks, copyrights or restricted rights notices in the systems, software and other materials used in the provision of Platform Services; or (iii) Access or use the Platform Services for the purpose of building competitive products or services by copying its features or user interface or by allowing a direct competitor of Accenture to access or use the Platform Services.

2.8 Client will notify Accenture immediately it becomes aware of any breach or threatened breach of the terms of this Section 2, or of any breach or threatened breach of security including any attempt by a third party to gain unauthorized access to the systems used for the provision of the Platform Services.

2.9 Client acknowledges and agrees that it is responsible for obtaining and maintaining all hardware, software, communications equipment and network connections necessary to access and use the Platform Services, and for paying any applicable third-party fees and charges incurred while accessing and using the Platform Services.

2.10 Client owns all right, title and interest in the Client Content or has the necessary Consents to enable Accenture to use the Client Content in providing the Services. Consents shall mean necessary consents, permissions, notices and authorizations necessary for Accenture to perform the Services, including valid consents from or notices to applicable data subjects (i.e. applicants, beneficiaries; employees) and authorizations from third parties, including regulatory authorities.

3 ACCENTURE'S RIGHTS AND OBLIGATIONS

3.1 Accenture shall provide the Platform Services in accordance with an executed Service Order. Accenture will also provide Support as set forth in the Service Order.

3.2 If the Parties so agree in any applicable Service Order, Accenture may also provide certain Implementation Services or Professional Services in connection with the Platform Services ("**Additional Services**").

3.3 Accenture will use accepted industry standard security technologies (e.g. encryption, password protection and firewall protection) in providing the Platform Services.

3.4 Accenture may need to apply updates or make changes to the Platform Services that it is providing pursuant to any Service Order, provided always that Accenture shall not be entitled to apply such updates or other changes in a manner that would make the Platform Services non-conforming with the applicable service descriptions, or otherwise materially diminish the scope or the quality of the service provided, unless such changes are necessary for Accenture to comply with any applicable laws. Accenture will notify the Client reasonably in advance of any planned changes to the Platform Services that have any material impact on Client's access to or use of the relevant service.

3.5 Client acknowledges and agrees that Accenture shall be permitted to monitor the Client's and its Authorized Users' access and usage of the Platform Services limited solely for the purposes of verifying Client's compliance with the terms of this Agreement and the applicable Service Order.

3.6 Client hereby acknowledges, accepts and agrees that Accenture may have to suspend Client's and/or its Authorized Users' right to access or use all or any portion of the Platform Services, or remove any relevant Client Content as described below: (i) where such access or use, or any Client Content (x) poses a security risk to or may otherwise adversely impact the Platform Services or (y) infringes or otherwise violates the rights or other interests of a third party, entails illegal or otherwise prohibited content or activities, or otherwise subjects Accenture to a potential liability; or (ii) where Accenture is required to do so under any applicable laws, or any court's or governmental body's order.

3.7 When allowed under the applicable laws and if otherwise reasonable under the circumstances (as determined by Accenture in its discretion), Accenture shall provide Client with a written notice prior to such suspension, and an opportunity to take steps to avoid any such suspension. Any suspension of Client's or its Authorized Users' right to access or use the Platform Services shall not release the Client from its obligations under this Agreement and any Service Order, including any obligation of paying the fees. Accenture's suspension right is in addition to Accenture's right to terminate this Agreement or any Service Order pursuant to Section 10.

4 CLIENT CONTENT

4.1 Client (and Client's licensors, where applicable) own all right, title and interest in and to the Client Content or has the necessary Consents to enable Accenture to use the Client Content in providing the Services.

4.2 Client acknowledges and agrees that it is solely responsible for complying with any regulations, laws, or conventions applicable to the Client Content. In particular, Client agrees that it is the principal and Accenture shall be its agent with respect to the Processing of all Client's Personal Information, on Client's behalf and in accordance with Instructions (as defined below) provided by the Client. Each party shall comply with their respective obligations as described above under applicable data privacy laws. This Agreement, the applicable Service Order, and reasonable instructions initiated by users of the Service consistent with the terms of the Agreement and Service Order consist of the full and complete instructions of the Customer ("Instructions").

In addition, Client is aware of Accenture's call recording technology, methodology and processes. if Client instructs Accenture to record calls or retain chatbot conversations using Accenture's technology ("Recordings") in connection with the Services as described in the applicable Service Order, Client represents and warrants that it will comply with all laws applicable to such Recordings and notify end customers and obtain and document end customer consent for such Recordings made by Accenture at the request of Client. Client has determined under all applicable laws in the jurisdiction(s) where end customers are located and/or where Recording activities will occur that Accenture can legally make such Recordings on Client's behalf.

4.3 Client grants to Accenture the nonexclusive right to host, store, process and transfer the Client Content solely for the purposes of Accenture's providing, and only to the extent necessary for Accenture to provide, the Platform Services and as otherwise set forth in this Agreement.

4.4 Client shall have the ability to access its Client Content hosted in the Platform Services at any time during the Term set forth in the applicable Service Order. Client may export and retrieve its Client Content during the said Term, subject to any technical limitations in the Platform Services or Client hardware and software (and that of its Authorized Users), including factors such as (i) the size of Client's instance of the Platform Services; and (ii) the frequency and/or timing of the export and retrieval.

4.5 Client is responsible for obtaining and maintaining all hardware, software and communications equipment necessary to access and use the Platform and for paying all third-party access charges (e.g., ISP, telecommunications) incurred while using the Platform.

4.6 Accenture may use usage patterns, trends, and other statistical data derived from use of the Platform Service by Authorized Users (but not Client Content itself) ("**Usage Data**") for the purposes of providing, operating, maintaining, or improving the Platform Services and any Accenture products and services used to deliver the Platform Services.

4.7 The applicable Service Order will indicate whether or not Accenture will have access to Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act of 1996, as amended from time to time. If no PHI applies, Schedule 2 herein shall be removed and reserved. Conversely, if PHI is accessed under this Agreement, prior to Accenture receiving access to such PHI, the parties will enter into a business associate agreement.

5 FEES, PAYMENTS AND TAXES

5.1 Client shall pay the fees specified in the applicable Service Order. Fees are stated exclusive of all applicable duties, tariffs, and taxes. Unless otherwise specified in a Service Order, fees will be due and payable within thirty (30) days of Accenture's invoice. Late payments that are not the subject of a good faith dispute are subject to an interest charge, which is the lesser of: (a) one and one-half percent (1.5%) per month, or (b) the maximum legal rate.

5.2 Client will provide any information reasonably requested by Accenture to determine whether Accenture is obligated to collect VAT and sales tax from Client, including Client's VAT and sales tax identification number. If Client is legally entitled to an exemption from any sales, use, or similar transaction tax, Client is responsible for providing Accenture with legally-sufficient tax exemption certificates for each taxing jurisdiction. Accenture will apply the tax exemption certificates to charges under Client's accounts occurring after the date Accenture receives the tax exemption certificates. If any deduction or withholding is required by applicable law, Client will notify Accenture and will pay any additional amounts necessary to ensure that the net amount that Accenture receives, after any deduction and withholding, equals the amount Accenture would have received if no deduction or withholding had been required. Additionally, Client will provide Accenture with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

5.3 Client will be responsible for the payment of all taxes in connection with this Agreement including, but not limited to, sales, use, excise, value-added, business, service, goods and services, consumption, withholding, and other similar taxes or duties, including taxes incurred on transactions between and among Accenture, its Affiliates, and third party subcontractors. Client will reimburse Accenture for any deficiency relating to taxes that are Client's responsibility under this Agreement. Each Party will be responsible for its own income taxes, employment taxes, and property taxes. The Parties will cooperate in good faith to minimize taxes to the extent legally permissible. Each Party will provide to the other Party any resale exemption, multiple points of use certificates, treaty certification and other exemption information reasonably requested by the other Party.

5.4 All amounts payable under this Agreement will be made without set-off or counterclaim, and without any deduction or withholding.

6 ACCENTURE'S INTELLECTUAL PROPERTY RIGHTS

6.1 Accenture (and its licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to the systems, software and other content and materials used in the provision of the Platform Services. In addition, Client agrees that Accenture (and its licensors, where applicable) will own all right, title and interest in and to any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Client or any other Party relating to the Platform Services, and Client hereby assigns any intellectual property rights in such items to Accenture. The Accenture name, the Accenture logo, and the product names associated with the Platform Services are trademarks of Accenture or third parties, and no right or license is granted to Client to use them.

6.2 Government Use. The Platform Services solution (individually and collectively with other materials provided by Accenture, (the "Solution") licensed under this Agreement is proprietary commercial computer software funded entirely at private expense. All right, title and interest in the Solution belongs solely and exclusively to Accenture. The parties expressly stipulate and agree that the Solution constitutes proprietary software under 45 CFR § 95.617(c) and shall be deemed as "commercial computer software" as that term is defined in 48 CFR 2.101. Any derivatives, modifications, changes, translations or fixes ("Derivatives") to the Solution and to the documentation shall be exclusively owned by Accenture, and Licensee shall be granted a license to such Derivatives as may be created during the course of any implementation or maintenance activity of the Solution on the same terms as the license granted for the Platform Services.

7 **WARRANTIES AND EXCLUSIONS**

7.1 Accenture warrants that the Platform Services provided to Client pursuant to this Agreement will comply in all material respects with the Documentation identified in the applicable Service Order. This warranty shall not apply where: (i) the Client's or any Authorized User's access or use of the Platform Services is not in accordance with this Agreement, the relevant Service Order (or any Exhibits to the relevant Service Order) or with Accenture's instructions; (ii) modification or alteration of the Platform Services or any systems, software or other content or materials embodied therein is made by any Party other than Accenture; or (iii) the Platform Services are being provided free of charge, or as a trial, pre-release or as a beta release.

7.2 Client shall provide Accenture with prompt written notice of any non-conformity of the Platform Services, sufficiently describing such non-conformity, no later than within thirty (30) days of the appearance or Client's discovery of such non-conformity.

7.3 In such event, Accenture will use commercially reasonable efforts to correct any such non-conformity. In the event Accenture is unable to correct such non-conformity by exercising commercially reasonable efforts for a reasonable period of time, either Party may terminate the relevant Service Order concerning the non-conforming Platform Service(s) on written notice to the other Party in which case as Client's sole and exclusive remedy, Accenture will provide a pro-rated refund of any pre-paid Fees for periods after the effective date of termination.

7.4 **Disclaimer.** EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 7, ACCENTURE, ITS AFFILIATES AND ITS LICENSORS MAKE NO REPRESENTATIONS AND PROVIDE NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE PLATFORM SERVICES OR ANY THIRD PARTY COMPONENTS OR CONTENT EMBODIED THEREIN, INCLUDING ANY WARRANTY THAT THE PLATFORM SERVICES WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING CLIENT CONTENT OR THIRD PARTY COMPONENTS OR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED, AND 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. EACH PARTY, ITS AFFILIATES AND ITS LICENSORS DISCLAIM ALL, AND THE OTHER PARTY AGREES THAT IT IS NOT ENTITLED TO ANY EQUITABLE OR IMPLIED INDEMNITIES. THESE DISCLAIMERS SHALL ONLY APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW.

7.5 **High Risk Activities.** Accenture, on behalf of itself and its Affiliates and licensors and the Cloud Vendor, specifically disclaims any express or implied warranty of fitness of the Platform Services for High Risk Activities.

8 **THIRD PARTY CLAIMS**

8.1 Subject to the limitations in Section 9, Accenture will defend (at its sole expense) Client and Client's Affiliates against any claims brought against Client by any third party (that is not an Affiliate of Client) alleging that Client's use of the Platform Services, in accordance with the terms and conditions of the Agreement and the applicable Service Order, constitutes a direct infringement of a patent issued in the United States as of the Effective Date, copyright, or trade secret of any third

party. Accenture will only be obliged to pay the amount of any damages finally awarded against Client or the amount of any settlement agreed by Accenture.

8.2 Accenture will have no obligations or liability under Section 8.1 for any claims to the extent arising from:

8.2.1 Client Content;

8.2.2 Client's or any Authorized User's use of the Platform Services after Accenture has notified Client, in accordance with this Agreement, to discontinue such use and Client have been afforded a reasonable opportunity to discontinue such use;

8.2.3 any unauthorized modification or unauthorized use of the Platform Services where infringement or misappropriation would not have occurred but for such unauthorized modification or unauthorized use;

8.2.4 any use of the Platform Services, or any other act, by Client or an Authorized User, that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for the breach;

8.2.5 any claim of wilful infringement adjudicated against anyone other than Accenture and its Affiliates or Cloud Vendor;

8.2.6 any combination(s) of the Platform Services with any other product, service, software, content, data or method not supplied by Accenture; or

8.2.7 a free (no fee) or trial license of the Platform Services.

8.3 If any portion of the Platform Services are alleged to infringe any third party Intellectual Property Rights, Accenture may choose (at its election and expense) to: (a) procure the rights to use the item alleged to be infringing; (b) replace the alleged infringing portion with a non-infringing equivalent; or (c) modify the alleged infringing portion to make it non-infringing while still providing substantially the same level of functionality. If Accenture determines the actions from Section 8.3 (a) to (c) are not commercially reasonable, Accenture may immediately terminate Client's access to the Platform Services.

8.4 Client shall defend (at its sole expense) Accenture and its Affiliates and licensors against claims brought against Accenture by any third party (that is not an Affiliate of Accenture) arising from or related to (i) any use of Platform Services by Client or its Authorized Users in violation of any applicable law or regulation; or (ii) any allegation that the Client Content violates, infringes or misappropriates the rights of a third party; (iii) Client's or its Authorized Users' use of the Platform Services or other act in violation of this Agreement or the relevant Service Order; or (iv) Client's or any Authorized User's engaging in High Risk Activities The foregoing shall apply regardless of whether such damage is caused by the conduct of Client and/or its Authorized Users or by the conduct of a third party using Client's or an Authorized User's access credentials where Client has negligently made the credentials available or chosen credentials that are easy to hack into. Client will only be obliged to pay the amount of any damages finally awarded against Accenture or the amount of any settlement agreed by Client.

8.5 Client will have no obligations of liability under Section 8.4 for any claims arising from:

8.5.1 Client Content after Client has notified Accenture, in accordance with the terms of this Agreement, to delete the Client Content from the SaaS and Accenture has been afforded a reasonable opportunity to do so; or

8.5.2 any unauthorized access or use of the Client Content by Accenture that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for such breach.

8.6 In connection with any third party claims pursuant to Section 8.1 or 8.4, the indemnified Party will (a) give the indemnifying Party prompt written notice of the claim; (b) reasonably cooperate with the indemnifying Party (at the indemnifying Party's expense) in connection with the defense and settlement of such claim, and (c) grant the indemnifying Party sole control of the defense and settlement of the claim, except that the indemnifying Party may not consent to the entry of any judgment or enter into any settlement with respect to the claim without the indemnified Party's prior written consent unless the settlement or judgment is purely financial, is paid entirely by the indemnifying Party, is confidential, does not require the indemnified Party to admit to any fault or wrongdoing, and fully releases the indemnified Party from any and all further claims or causes of action relating to the subject matter of the claim. The non-controlling Party may, at its expense, participate in the defense and settlement of the claim with counsel of its own choosing. In the event that the indemnifying Party fails to assume control within 30 days of written notice of the claim, the indemnified Party may assume control of the defense of the claim

8.7 **Exclusive Remedy**. SECTION 8.1 CONSTITUTES CLIENT'S SOLE AND EXCLUSIVE REMEDY AND ACCENTURE'S (AND ITS AFFILIATES') ENTIRE OBLIGATION TO CLIENT WITH RESPECT TO ANY CLAIM THAT THE PLATFORM SERVICES INFRINGE OR MISAPPROPRIATE THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

9 **LIMITATION OF LIABILITY**

9.1 EXCEPT FOR: (I) DAMAGES RESULTING FROM A BREACH OF A PARTY'S OBLIGATIONS IN SECTION 11 WITH RESPECT TO CONFIDENTIAL INFORMATION; (II) DAMAGES RESULTING FROM DEATH OR BODILY INJURY ARISING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OR FROM FRAUD OR FRAUDULENT MISREPRESENTATION; AND (III) ACCENTURE'S RIGHT TO COLLECT UNPAID FEES DUE HEREUNDER, UNDER NO CIRCUMSTANCES AND REGARDLESS OF THE NATURE OF ANY CLAIM SHALL EITHER PARTY (OR THEIR RESPECTIVE AFFILIATES OR ACCENTURE'S LICENSORS) BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY UNDER THE AGREEMENT FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID FOR THE APPLICABLE PLATFORM SERVICE IN THE TWELVE (12) MONTH PERIOD PRECEDING THE DATE OF THE INCIDENT GIVING RISE TO LIABILITY.

9.2 TO THE EXTENT PERMITTED BY LAW NEITHER PARTY NOR ANY OF EITHER PARTY'S RESPECTIVE AFFILIATES WILL BE LIABLE TO THE OTHER PARTY UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF

THE POSSIBILITY OF SUCH DAMAGES, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES; BUSINESS INTERRUPTION, LOSS OF PROFITS OR SAVINGS, REVENUES, OR GOODWILL; LOSS OR CORRUPTION OF DATA; UNAVAILABILITY OF ANY OR ALL OF THE PLATFORM SERVICES; INVESTMENTS, EXPENDITURES OR COMMITMENTS RELATED TO USE OF OR ACCESS TO THE PLATFORM SERVICES; COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; UNAUTHORIZED ACCESS TO, COMPROMISE, ALTERATION OR LOSS OF CLIENT CONTENT OR BUSINESS INFORMATION; OR COST OF REPLACEMENT OR RESTORATION OF ANY LOST OR ALTERED CLIENT CONTENT.

9.3 The Parties acknowledge that the limitations on liability set out in this Section 9 are essential terms of this Agreement and the Parties would not have entered this Agreement without them.

9.4 No action, regardless of form, arising out of this Agreement may be brought by Client more than two (2) ears after Client knew or should have known of the event which gave rise to the cause of action.

10 **TERM AND TERMINATION**

10.1 The term of this Agreement will commence on the Effective Date and will continue until terminated by either Party pursuant to this Section 10 ("**Term**"). The term of any Service Order shall be agreed in the Service Order itself, and the terms and conditions of this Agreement shall survive and remain in force to govern any Service Order the term of which exceeds any termination of this Agreement.

10.2 Either Party may terminate this Agreement (but not a Service Order) for convenience upon sixty (60) days written notice to the other Party. For the avoidance of doubt, either Party may only terminate a Service Order in accordance with the terms of the Service Order or as expressly provided for in this Agreement.

10.3 Either Party may terminate this Agreement and/or any Service Order upon written notice if the other Party ceases its business operations or becomes subject to insolvency proceedings or any similar or equivalent process in any jurisdiction, and the proceedings are not dismissed within ninety (90) days, or otherwise becomes generally unable to meet its obligations under this Agreement and/or the Service Order.

10.4 In addition to any other remedies that a Party may have at Law, in equity, or under this Agreement, a Party may terminate this Agreement and/or any Service Order upon thirty(30) days' advance written notice to the other Party if the other Party commits any material breach of this Agreement and/or any Service Order and fails to cure such default (if curable) within the thirty (30) day period, including if there has been any such act or omission by Client or any Authorized User that has given Accenture the right to suspend the provision of Platform Services in accordance with Section 3.6.

10.5 Accenture may also terminate this Agreement and/or any Service Order without liability upon thirty (30) days' notice to Client or any Authorized User: (i) in the event where an underlying contract between Accenture and the Cloud Vendor concerning the provision of the IaaS terminates, or (ii) if termination of the Agreement and/or any Service Order is necessary to comply with applicable law or binding requests of governmental entities.

10.6 Upon the effective date of expiration or termination of a Service Order, Accenture shall immediately cease Client's and its Authorized Users' access to and use of the Platform Services.

10.7 Where so agreed in the applicable Service Order, Accenture will provide Client with the ability to retrieve Client Content after the expiry or termination of the said Service Order for a limited period of time, in which instance the Client will cover the costs of the data storage unless otherwise agreed in the Service Order. Otherwise, Accenture may destroy (or procure the destruction of) or otherwise dispose of any Client Content in its possession or that of a Cloud Vendor (including any data back-ups) upon expiry or termination of the applicable Service Order.

10.8 If so mutually agreed in the Service Order, Accenture shall provide to Client reasonable co-operation and assistance to facilitate the orderly wind down of the usage of the Platform Services and/or to assist Client to transition to another provider. Client will pay Accenture for such assistance at Accenture's then-current time and materials rates for the applicable services or as otherwise mutually agreed by Client and Accenture. If the termination results from a breach of this Agreement by Client, Accenture may invoice Client in advance for all transition assistance services and, if so invoiced, Client will pay in advance.

11 **CONFIDENTIALITY**

11.1 Each Party agrees that it will use the other Party's Confidential Information only to the extent reasonably necessary for purposes of this Agreement or a Service Order. Each Party agrees to take reasonable steps to protect the other's Confidential Information, provided that these steps must be at least as protective as those the Party takes to protect its own Confidential Information of similar nature, but in any event no less than a reasonable standard of care.

11.2 Each Party may disclose the other Party's Confidential Information to its Affiliates, employees, contractors, licensors and agents who: (a) have a need to know it for purposes contemplated by this Agreement, and (b) are legally bound to protect the Confidential Information on terms no less protective than the terms of this Agreement.

11.3 This Section 11 will not apply to any information that either Party can demonstrate: (a) was at the time of disclosure or that has become thereafter published or otherwise becomes publicly available at no fault of the receiving Party; (c) was in the possession of the receiving Party at the time of disclosure to it and was not the subject of a pre-existing confidentiality obligation; (d) was received after disclosure to it from a third party who had a lawful right to disclose such information

(without corresponding confidentiality obligations) to it; or (e) was independently developed by the receiving Party without use of the Confidential Information of the disclosing Party.

11.4 The receiving Party will not be considered to have breached its obligations under this Section 11 for disclosing Confidential Information of the disclosing Party to the extent required to satisfy any legal requirement of a competent governmental or regulatory authority, provided that promptly upon receiving any such request and to the extent that it may legally do so, the receiving Party: (i) advises the disclosing Party prior to making such disclosure in order that the disclosing Party may object to such disclosure or take any other action that it considers appropriate to protect the Confidential Information and; (ii) takes actions necessary to minimize any disclosure to only that necessary to satisfy any legal requirement of a competent governmental or regulatory authority (including through redaction of sensitive commercial information, where legally permissible).

11.5 Any reproduction of any Confidential Information of the other Party shall remain the property of the disclosing Party, and the disclosing Party may, at any time including on termination or expiration of this Agreement, request the receiving Party to return, destroy or delete (and confirm the destruction or deletion of the same) as instructed (in such a manner that it cannot be recovered) all Confidential Information of the disclosing Party in the receiving Party's possession or control. Notwithstanding the foregoing, each Party may archive all copies of Confidential Information that it is required to retain to comply with law and its other record-keeping requirements.

11.6 Client shall not disclose the terms and conditions of this Agreement or the pricing contained herein to any third party unless otherwise agreed by the Parties. Neither Party will use the name of the other Party without the prior written consent of the other, except that Client agrees that Accenture may use Client's name in customer listings or quarterly calls with its investors or, at times mutually agreeable to the parties, as part of Client's marketing efforts (including reference calls and stories, press testimonials, and prospective customer meetings).

12 **ADDITIONAL TERMS**

12.1 **Compliance with Export Control Laws.** Each Party will comply with all export control and economic sanctions laws applicable to its performance under this Agreement. Client agrees that Client will and will procure that Authorized Users do not use the Platform Services in or in relation to any activities involving a country subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria or the Crimea region of Ukraine), or involving a Party in violation of such applicable trade control laws, or that require government authorization, without first obtaining the informed consent of Accenture and the required authorization. For the avoidance of doubt, Client shall not grant access to the Platform Services to any individual, entity or organization which is subject to trade sanctions or embargos by the United States or any applicable jurisdiction, including any individual, entity or organization which is listed on the OFAC Specially Designated Nationals List from time to time.

12.2 **Notices**. Unless expressly stated otherwise in this Agreement, all notices under this Agreement must be in writing and must be delivered personally, sent by certified mail (return receipt requested); or sent by express courier (with confirmation of delivery). The notice will be deemed given and will be effective upon receipt: (a) when it is delivered to a Party personally; (b) upon receipt if sent certified mail, return receipt requested; or (c) when delivered by a nationally recognized overnight courier service such as FedEx (with confirmation of delivery). Any notice by email will only be allowed in the particular Sections of this Agreement that expressly permit it. All notices must be addressed to the other Party at the address set forth in the preamble above. Either Party may designate a different address by giving ten (10) days' written notice to the other Party in accordance with this Agreement. A copy of any notice under the terms of this Agreement (except for invoices and other routine correspondence) will be forwarded to: Accenture LLP, Legal – General Counsel, 161 North Clark Street, Chicago, Illinois 60601. Such copy will not constitute effective notice. All communications and notices to be made or given pursuant to this Agreement must be in the English language.

12.3 **Governing Law and Jurisdiction**. The laws of [the State of Illinois and federal laws of the United States] will govern the construction, validity and operation of this Agreement and the performance of all obligations hereunder without regard for Illinois' choice of law provisions. The courts of Chicago, Illinois shall have exclusive jurisdiction in relation to any dispute or matter arising under or in connection with this Agreement.

12.4 **Force Majeure**. Other than Client's obligation to pay Accenture pursuant to this Agreement and any Service Order, neither Party will be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond its reasonable control, including but not limited to electrical or power outage, utilities or telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war, or labour disputes with its or its affiliates' employees, industrial disturbances.

12.5 **Survival**. The provisions of Sections 6, 7.4, 8, 9, 11 and 12, and any other Sections which by their nature are intended to survive, will survive the termination or expiration of this Agreement.

12.6 **Assignment**. Client may not assign this Agreement or delegate or sublicense any of Client's rights or obligations hereunder, including by operation of law, without the prior written consent of Accenture and any attempt to do so in violation of this

provision will be null and *void*. This Agreement will be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns.

12.7 **Variation**. Except as otherwise expressly provided to the contrary in this Agreement, this Agreement may only be changed, modified or expanded by a writing signed by both Parties.

12.8 **No waiver**. No delay, neglect or forbearance on the part of either Party in enforcing against the other any term or condition of this Agreement will be deemed to be a waiver nor will it in any way prejudice any right of that Party under this Agreement nor will any single or partial exercise of any right preclude any other or further exercise of these rights or any other right.

12.9 **Severability**. The invalidity or unenforceability of any provision of this Agreement will not affect the validity or enforceability of any other provision hereof and it is the intent and agreement of the Parties that this Agreement will be deemed amended by modifying such provision to the extent necessary to render it valid, legal and enforceable while preserving its intent or, if such modification is not possible, by substituting another provision that is legal and enforceable and that achieves the same objective. The Parties agree that any principle of construction or rule of law that provides that an agreement will be construed against the drafter will not apply to this Agreement.

12.10 **Entire Agreement**. This Agreement, along with any Service Orders, attachments, exhibits, Attachments or referenced documents or agreements attached hereto from time to time, contains the entire Agreement between the Parties with respect to the matters specified herein and supersedes all prior or contemporaneous representations, understandings, agreements or communications between Accenture and Client, whether written or verbal, regarding the subject matter of this Agreement.

12.11 **Relationship of the Parties**. Nothing in this Agreement will be deemed to create a joint venture, partnership, or agency relationship between the Parties or be deemed to authorize either Party to incur any liabilities or obligations on behalf of, or in the name of, the other.

12.12 **Third Party Rights**. Accenture's licensors are third party beneficiaries hereunder. This Agreement does not otherwise create any third party beneficiary rights, and in particular it is agreed that Client's Authorized Users are not third party beneficiaries. Accenture and Client are independent contractors.

12.13 **Existing Agreements**. This Agreement is separate from any obligations, rights, or requirements contained in any existing master services agreement, professional services agreement, consulting services agreement, outsourcing agreement, or related agreements ("**Existing Agreements**") between the Parties. Any Existing Agreement will not apply to the products and services that are the subject of this Agreement, and this Agreement expressly overrides any conflicting statements in any Existing Agreement.

12.14 **Counterparts.** This Agreement may be executed in any number of counterparts and executed by facsimile or by other electronic communication as agreed upon by the Parties, such execution to be considered an original for all purposes, and all of which together will constitute one and the same instrument, notwithstanding that the Parties may not both be signatories to the original or same counterpart.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly Authorized representatives and caused it to be effective as of the date first written above.

ACCENTURE:	**Client:** _____
BY:_____	BY:_____
PRINTED NAME: _____	PRINTED NAME: _____
TITLE: _____	TITLE: _____
DATE:_____	DATE: _____

EXHIBIT A
DEFINITIONS

"**Additional Services**" has the meaning given to it in Section 2;
"**Affiliate**" of a Party means any entity, whether incorporated or not, that is Controlled by, Controls, or is under common Control with such Party. "Control" means the ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise;
"**Agreement**" means this Accenture Platform Services Agreement, any exhibits attached hereto and any other documents incorporated hereto by reference, together with any amendments hereto duly executed by the Parties;
"**Authorized User**" means any individual or entity that, directly or indirectly through another Authorized User, accesses or uses the Platform Services;
"**Cloud Vendor**" means the relevant cloud service provider, providing the IaaS;
"**Client Content**" means any content, materials, data and information, including Personal Information that Client or its Authorized Users enter into the Platform Services. Client Content shall not include any component of the Platform Services or material provided by or on behalf of Accenture.
"**Confidential Information**" means information that relates to the other Party's (or to Cloud Vendor's) past, present, or future research, development, business activities, products, services, and technical knowledge, which is identified by the discloser as confidential or that would be understood to be confidential by a reasonable person under the circumstances. For the purposes of this Agreement, the term "Confidential Information" does not include Client Content;
"Consents" shall mean necessary consents, permissions, notices and authorizations necessary for Accenture to perform the Platform Services, including valid consents from or notices to applicable data subjects (i.e. applicants, beneficiaries; employees) and authorizations from third parties, including regulatory authorities.
"**Effective Date**" means the date first written above;
"Documentation" means the description of the Platform Services contained in the Service Order.
"**Fees**" means the fees specified in the relevant Service Order and payable in accordance with Section 6 or the relevant Service Order;
"**High Risk Activities**" means Usage such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems environments where the use or failure of the Service could lead to death, personal injury or environmental damage;
"**IaaS**" means the infrastructure-as-a-service provided by a Cloud Vendor on which the Platform Services are hosted or is otherwise utilized in the provision of the Platform Services by Accenture;
"**Intellectual Property Rights**" means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights, derivatives thereof, and forms of protection of a similar nature;
"Permitted Purpose" shall have the meaning set forth in the Service Order.
"**Personal Information**" means data which names or identifies a natural person including, without limitation: (a) data that is explicitly defined as a regulated category of data under data privacy laws applicable to Client; (b) non-public personal data, such as national identification number, passport number, social security number, driver's license number; (c) health or medical information, such as insurance information, medical prognosis, diagnosis information or genetic information; (d) financial information; and/or (e) sensitive personal data, such as race, religion, marital status, disability, or sexuality;
"**Platform Services"** or **"Platform"** means a hosted solution comprising the integration of robotic process automation technology, artificial intelligence and machine learning technology, natural language processing technology, algorithms, processes and software to enable the foregoing, corresponding documentation, made available by Accenture for Client's access and use on a subscription basis, as detailed in the applicable Service Order. The term "Platform Services" includes any modifications, enhancements, additions, extensions, translations and derivative works thereof and any configuration and related services. The Platform Services do not include Client Content or any Client-provided third-party software;
"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"**Service Order"** means the documents referenced in Section 1.2, and its Schedules, and any other documents incorporated by reference herein, together with any amendments thereto duly executed by the Parties, A Service Order template is attached as Exhibit B;
"**Term**" has the meaning set forth in Section 10;
"**Usage Data**" has the meaning set forth in Section 4.6;
"**Virus**" means any item, software, device or code which is intended by any person to, or which is likely to, or which may:

(a) impair the operation of any software or computer systems;
(b) cause loss of, or corruption or damage to any software or computer systems or data;
(c) prevent access to or allow unauthorised access to any software or computer system or data; and / or
(d) damage the reputation of the Client and / or Accenture, including any computer virus, Trojan horse, worm, software bomb, authorization key, license control utility or software lock.

Exhibit B

Service Order Template

SERVICE ORDER

To ACCENTURE VIRTUAL ASSISTANT PLATFORM AGREEMENT
Terms and Conditions

This Service Order is entered into by and between [Accenture] and [Client] for the provision of the Platform, as further detailed below. This Service Order is effective upon the signature below by both Parties ("Service Order Effective Date").

This Service Order is subject to and incorporates the terms and conditions of the Accenture Virtual Assistant Platform Agreement ("Agreement") entered into by the parties on [add date]. Unless otherwise defined in this Service Order, all capitalized terms will have the same meanings as set forth in the Agreement.

This Service Order includes the following Schedules:

- Schedule 1 - The Platform (Configuration, Fees and Support)
- Schedule 2 – Business Associate Addendum (if applicable)

1. **Definitions**

"Permitted Purpose" means [PLEASE PROVIDE]

2. Use of the Platform

a. Client will make the Client Content available for in the Platform. The Platform's configuration, applicable Fees, standard support services and related terms are described in Schedule 1.
b. Client may use the Platform for its and its Affiliates' internal purposes and consistent with the Permitted Purpose. Client is responsible for obtaining any third-party software (e.g., Tableau Reader) that may be needed with the Platform.

2. **Security Standards**

Accenture maintains a standard information security program (including the adoption and enforcement of internal policies and procedures) applicable to all AIP clients designed to (i) identify reasonably foreseeable and internal risks to security and unauthorized access to the Platform network, and (ii) minimize security risks, including through risk assessment and regular testing. The program includes the use of accepted industry standard security technologies (e.g. encryption, password protection and firewall protection) in connection with AIP ("Security Standards"). A description of the program is provided separately.

3**. Terms Applicable to Certain Regulated Sectors**.

a. Health Sector:
(i) [OPTION A] The parties shall comply with the Business Associate Addendum attached to this Attachment as **Schedule 2**, as applicable. [OPTION B] Client warrants and represents that it will not provide any protected health information (as defined in 45 CFR 160.103 of the US Health Insurance Portability and Accountability Act) to Accenture in connection with this Agreement. If Client wishes to provide any such protected health information, Client shall contact Accenture to request this and the terms related to the provision of a HIPAA account. *[DRAFTING NOTE: Option A should only be used if the Client Content certain data that is protected health information under the US HIPAA legislation, in which case the addendum in Attachment C must be signed. Otherwise, Option B can be used and Attachment C removed.]*
(ii) The Platform and Platform Outputs are not intended to be used: (i) to prevent, diagnose or treat health or medical conditions, (ii) to monitor health or medical conditions for purposes of prevention or treatment of health or medical conditions, or (iii) as a medical device, medical application or medical monitoring platform. Further, the Platform and Platform Outputs have not been evaluated by the Food and Drug Administration or similar regulatory agency for safety or effectiveness. Client will be responsible to ensure that any services or products Client offers or sells in reliance on the Platform or Platform Outputs are sold, marketed and distributed in compliance with all applicable Laws, including FDA, FTC and ONC regulations.

b. Other Regulated Sectors:

[Each deal team to identify]

c. General:
   (i) Client shall be responsible for making eligibility determinations based on its eligibility criteria for Client's public assistance programs.

4. **Professional Services**.

Accenture will perform professional services, if any, as specified below in accordance with the terms set forth in Schedule 3. These may include, without limitation, consulting, systems integration, designing client-specific dashboards, or creating other client-specific applications or models).

Description of additional services to be provided:

Services: Deliverables: Fees:

6. Term and Termination

a. Service Order Term: as set forth in Schedule 1.

b. Post termination assistance: Client may retrieve Client Content from the Cloud Vendor during a 60-day period following termination of this Service Order. Any additional post-termination assistance from Accenture is subject to mutual agreement of the parties. Client will pay for any post-termination use of the Infrastructure Services, including applicable data storage fees. Accenture will not be obligated to provide the post-termination assistance described in this Section where: (A) it is prohibited by applicable law or the order of a governmental or regulatory body; or (B) Accenture reasonably anticipates liability arising from such assistance, or (C) Client has not paid all undisputed amounts due under this Service Order. Accenture shall notify Client if it intends not to provide post-termination assistance because of circumstances described in (A) or, (B), or (C).

IN WITNESS WHEREOF, the Parties have caused this Service Order to be executed by their duly authorized representatives and caused it to be effective as of the date first written above.

ACCENTURE:	**CLIENT:** _____
BY:_____	BY:_____
PRINTED NAME: _____	PRINTED NAME: _____
TITLE: _____	TITLE: _____
DATE:_____	DATE: _____

SCHEDULE 1

Platform (Configuration, Fees and Support)

Description of the Platform:

The Platform integrates industry-leading artificial intelligence and robotic process automation tools to provide Accenture's Health & Human Services customers a solution to help increase case worker capacity and transform service delivery. Users of the platform may interact with the virtual assistants through a variety of channels including voice, chat as well as text messages. A service orchestration engine (SOE) is the centerpiece to integrate the natural language understanding capabilities of the Platform with robotic process automation. The Platform is able to understand the intent of a user request, and through the SOE, respond appropriately by either corresponding directly to the user, calling custom or commercial API's or web services, or invoking an RPA process to complete automated actions in one or more systems. The Platform also offers analytics to gain insights into the usage and to measure the performance of the Platform's operations.

All components of the Platform are deployed in the cloud with appropriate security provisions . All data is encrypted both in transmission and at rest to allow protection of Personal Information All components are load balanced to provide for optimal performance and ease of scalability during periods of high demand.

Configuration:

[Business team to provide]

Fees:

[Business team to provide]

Support:

[Business team to provide]

SCHEDULE 2

Business Associate Addendum | RESERVED

[To be provided, only if applicable. Note that the BAA may be different based upon the Cloud Vendor.]

IF NOT APPLICABLE – REMOVE SCHEDULE AND ENTITLE IT AS: **RESERVED.**

SCHEDULE 3

Professional Services

Accenture will provide the services ("Services") and deliverables ("Deliverables") as specified in the Service Order, under the following terms and conditions:

1. **Payment**. Accenture will, at the beginning of each month, invoice Client for the fees for that month, plus any applicable out-of-pocket expenses; any necessary adjustments to the actual fees or expenses incurred will be made in the next month's invoice. Billable expenses will be billed at actuals or capped as specified in the Service Order. Expenses will be pre-approved by Client and will be invoiced at Accenture's actual cost. All invoices submitted to Client for payment will be itemized in reasonable detail and in line with Client's travel policies (provided separately). Payment for undisputed fee amounts is due within 30 days after Client's receipt of each invoice. Should any invoice (excluding disputed amounts) remain unpaid for more than 30 days, interest will be paid at a rate of 1% per month or the highest rate allowed by law, whichever is less. Any taxes arising out of this Agreement other than those on Accenture's net income will be Client's responsibility. Accenture will pay any taxes remitted to it by Client to the applicable taxing authority when due. The Service Order may further specify varied or other payment structures.

2. **Acceptance**. All Services and Deliverables will be deemed accepted if Client does not reject the Services and Deliverables by providing written notice within 10 business days after delivery specifically identifying the manner in which the Services or Deliverables fail to materially comply with their applicable specifications. Deliverables will be those items created for Client by Accenture which are specified in the Service Order.

3. **Materials**. All data, information, text, graphics, photos, designs, trademarks, logos or other artwork and materials provided to us by Client under this Agreement ("Client Materials") are and will remain the sole and exclusive property of Client or Client's third-party licensors and Client will obtain any relevant consents and licenses necessary for Accenture to use Client Materials to perform Services and provide Deliverables under this Agreement. Client hereby grants to Accenture, during the term of this Agreement, a non-exclusive, fully paid, non-transferable, limited license to use and permit our subcontractors to use the Client Materials. Upon final payment, Accenture hereby grants to Client a perpetual, worldwide, nontransferable, non-exclusive, irrevocable right and license to use, copy, modify and prepare derivative works of the Deliverables for purposes of Clients and Client's Affiliates' internal business only. All other rights in the Deliverables remain with and are assigned to Accenture. Accenture's software, data, tools, materials, or property existing prior to the Services, used in the Services, developed separately, or licensed to Accenture by third parties and used in the Services, and any enhancements or modifications to the same, are Accenture's sole and exclusive property ("Accenture's Property"). Accenture's Property embedded in Deliverables may not be used separately or beyond the license rights noted above. Subject to obligations of confidentiality in the Agreement, each party will be free to use the concepts, techniques and know-how retained in the unaided memories of those involved in the performance or receipt of the Services. In no event will Accenture be precluded from independently developing for Accenture, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the Deliverables provided and to the extent that they do not contain Client's Confidential Information. Within 10 business days after termination of this Agreement for any reason, Accenture will return any Client Materials in Accenture's possession to Client (subject to retaining copies of any information required for internal recordkeeping requirements). Third-party intellectual property, such as the licensing of third-party assets or third-party components, may require additional terms of usage.

4. **Warranties**. Accenture warrants that its Services will be performed in a good and workmanlike manner, in accordance with this Agreement. Accenture will re-perform any work not materially in compliance with this warranty brought to its attention within 30 days after that work is performed. THE PRECEDING ARE THE ONLY EXPRESS WARRANTIES CONCERNING THE SERVICES, ANY DELIVERABLES OR MATERIALS, OR THIS AGREEMENT, AND ARE MADE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, CONDITIONS AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, INFORMATIONAL CONTENT, SYSTEMS INTEGRATION, NON-INFRINGEMENT, INTERFERENCE WITH ENJOYMENT OR OTHERWISE.

5. **Indemnities**. Sections 8.1 through 8.3, 8.7 and 8.8 will apply to any Deliverables provided by Accenture to Client hereunder. Sections 8.4 through 8.7 will apply to Client's use of the Deliverables and to its provision of Client Materials.

SOFTWARE LICENSE AND MAINTENANCE SERVICES AGREEMENT

[NAME OF LOCAL ACCENTURE ENTITY] ("Accenture") will provide the software and Maintenance Services to _____ ("Client") as specified in separately signed schedules ("Schedules") under the following terms and conditions (collectively the "Agreement").

1. SOFTWARE LICENSE TERMS. Subject to Client's payment of the license fee and compliance with the terms of this Agreement, Accenture grants Client a non-exclusive, limited license for the license term defined in the Schedule to use and install the object code version of the Accenture software listed in the applicable license Schedule ("Software") and its documentation. All rights to the Software not expressly granted to Client under this Agreement are reserved to Accenture. Accenture will make the Software available to Client by electronic download. Client may make a reasonable number of copies of the Software for back-up and test purposes provided Client reproduces all ownership notices. Client may permit third parties to use the Software (a) solely as required for Client's own benefit and internal business purposes and (b) in compliance with the terms of this Agreement. Client is liable for all users' compliance with the terms of this Agreement. Client may not (a) use, distribute, copy, or modify the Software except as expressly permitted by this Agreement; (b) translate or attempt to reverse engineer, decompile, or make derivative works of the Software; or (c) sublicense, lease, or otherwise permit use of the Software for the benefit of a third party. Client will use the Software in compliance with its documentation (including any operating or security procedures and the hardware, software or networking requirements set forth therein).

2. MAINTENANCE SERVICES. Subject to Client's timely payment of the applicable maintenance fees, Accenture will make available the following maintenance services ("Maintenance Services"):

2.1 Technical Support. Technical support consists of (i) access to Accenture's support help desk for Error reporting; (ii) attempted diagnosis of reported issues in supported Software and (iii) reasonable commercial efforts to resolve reported Errors in supported Software that is implemented in accordance with the technical documentation. An "Error**"** is a verifiable failure of the unaltered Software to materially conform to the technical documentation. Technical support is limited to one production and one non-production instance of the Software.

2.2 Updates. Accenture will make available to Client any Updates. An "Update" means a subsequent Software release created at Accenture's discretion which Accenture generally makes available to active Maintenance Service customers for no additional license fee. Client is responsible for downloading and implementing any Update (including security Updates) and for making changes to their technical environment as necessary to use the Update.

3. FEES AND PAYMENT. Accenture will invoice Client for the license and Maintenance Services fees specified in the applicable Schedules. Should any invoice (excluding disputed amounts) become overdue by more than thirty (30) days, interest will be charged at a rate of 1% per month or the highest rate allowed by law, whichever is less from the original invoice due date, until the overdue balance is settled. Any taxes arising out of this Agreement other than those on Accenture's net income will be Client's responsibility. Accenture will pay any taxes remitted to it by Client to the applicable taxing authority when due. The Parties agree to cooperate to help enable each party to accurately determine and reduce its own tax liability and to minimize any potential liability to the extent legally permissible.

4. INTELLECTUAL PROPERTY. Accenture and its licensors, where applicable, own all right, title and interest, unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, know-how and other trade secret rights, and all other intellectual property rights, including derivatives, modifications, and enhancements thereof in all forms anywhere in the world ("Intellectual Property Rights"), in and to the Accenture Software and Maintenance Services and any suggestions, enhancement requests, feedback, or recommendations provided by Client or any other party relating thereto. The Software may also contain third-party open source components separately licensed under an open source license made available to Client with the Software. This Agreement does not convey to Client any rights in or related to the Software or the Maintenance Services or the Intellectual Property Rights owned by Accenture except as explicitly provided in this Agreement.

5. CONFIDENTIALITY. Each party may have access to information (in any form) that relates to the other party's past, present, and future activities including research, development, business activities, products, services, processes, and technical knowledge, which is identified by the disclosing party as confidential or reasonably understood to be confidential ("Information"). Information may only be used by the receiving party consistent with the rights and obligations of this Agreement. Information includes the Software and any related documentation made available to Client. The receiving party agrees to protect the Information of the disclosing party in the same manner that it protects its own similar confidential information, but in no event using less than a reasonable standard of care. Access to the Information will be restricted to Accenture and Client personnel (including such

personnel employed by their affiliates) and subcontractors with a need to use such Information pursuant to the parties' rights and obligations under this Agreement, provided such parties are bound by substantially similar obligations of confidentiality and are not listed as a competitor in the applicable Schedule. Accenture may retain and use Information relevant to its business purposes (including to provide or enhance its services) so long as its use of such Information is in an aggregated and anonymized or pseudonymized manner. Nothing in this Agreement will prohibit or limit either party's use of Information (i) previously known to it without an obligation not to disclose such information, (ii) independently developed by or for it without use of Information, (iii) acquired by it from a third party which was not, to the receiver's knowledge, under an obligation not to disclose such information, or (iv) which is or becomes publicly available through no breach of this Agreement.

6. LIMITED WARRANTY

6.1 Limited Warranty. Accenture warrants (i) that for a period of sixty (60) days from commencement of the initial license term defined in the Schedule ("**Warranty Period**") the Software as delivered will materially conform to Accenture's technical documentation made available for download or provided with the Software; and (ii) the Maintenance Services will be performed in a good and workmanlike manner. The warranties set forth in this Section are contingent upon Client's use of the Software in compliance with this Agreement and Client notifying Accenture of any such non-conformance during the applicable Warranty Period.

6.2 Remedy. Accenture will use commercially reasonable efforts to correct any non-conformance of the Software with the above warranty, If Accenture is unable to correct non-conformance of the Software as provided in 6.1 (i) above, Client will have the option as its exclusive remedy, to: (a) continue to use the Software pursuant to the terms of this Agreement, or (b) terminate the applicable Schedule and receive a refund of the license fee paid thereunder. As Client's exclusive remedy for any breach of the limited Maintenance Services warranty set forth in Section 6.1 (ii) above, Accenture will re-perform the Maintenance Service not in compliance with such limited warranty brought to Accenture's attention within thirty (30) days of Accenture's performance of such service.

6.3 No Other Warranties. THE WARRANTIES SET FORTH IN THIS SECTION 6 ARE THE ONLY WARRANTIES CONCERNING THE MAINTENANCE SERVICES, ANY SOFTWARE OR MATERIALS, OR THIS AGREEMENT, AND ARE MADE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, CONDITIONS AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, INFORMATIONAL CONTENT, SYSTEMS INTEGRATION, NON-INFRINGEMENT, INTERFERENCE WITH ENJOYMENT OR OTHERWISE. NO WARRANTY IS MADE THAT USE OF THE SOFTWARE WILL BE UNINTERRUPTED, ERROR FREE, OR THAT ANY ERRORS OR DEFECTS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE'S FUNCTIONALITY WILL MEET CLIENT'S REQUIREMENTS. CLIENT ACCEPTS RESPONSIBIILTY FOR ITS DATA AND THE SELECTION OF THE SOFTWARE TO ACHIEVE ITS INTENDED RESULTS.

7. INDEMNITY. Accenture will defend the Client, its parents, subsidiaries, affiliates, successors, and their directors, officers, employees, agents and representatives (collectively the "Indemnified Parties"), from and against any and all third party claims, demands, lawsuits, judgments, fines, and penalties (including interest thereon and court costs) caused by a claim that the Software maintained pursuant to the Maintenance Services ("Indemnified Claims") (i) infringes a third party's copyright, trademark or US patent existing as of the date of delivery of such Software or (ii) misappropriates a third-party's trade secrets Accenture will have no liability, however, to any Indemnified Party to the extent the alleged infringement or misappropriation was caused by: (I) modifications to the Software; (II) use of the Software in combination with any hardware or software not delivered by Accenture under this Agreement or specified in the technical documentation for the Software; (III) the failure of an Indemnified Party to implement corrections or enhancements to the Software made available by Accenture; (IV) use of the Software not explicitly authorized under this Agreement. If any Software is, or in Accenture's opinion is likely to be, held to be infringing, Accenture will at its expense and option either: (i) procure the right for Client to continue using it, (ii) replace it with a non-infringing equivalent, (iii) modify it to make it non-infringing, or (iv) direct the return of the Software and refund to Client the license fees paid for such reduced on a pro-rated basis by 20% of the original license fee amount for each year since the license schedule execution date. This section sets forth the sole and exclusive remedies for Indemnified Claims. To receive the benefits of this provision, the Indemnified Party must promptly notify the Indemnifying Party in writing of any eligible claim or demand and provide the Indemnifying Party reasonable cooperation and full authority to defend or settle same provided that such settlement does not impose any obligation (monetary or otherwise) on the Indemnified Party without its consent.

8. LIMITATION OF LIABILITY. EXCEPT FOR A BREACH BY EITHER PARTY OF: (A) THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (B) ITS INDEMNIFICATION OBLIGATIONS; OR (C) ITS PAYMENT OBLIGATIONS, EACH PARTY'S SOLE LIABILITY TO THE OTHER FOR ANY AND ALL CLAIMS RELATING TO (i) A LICENSE SCHEDULE SHALL BE LIMITED IN THE AGGREGATE TO THE LICENSE FEES PAID BY CLIENT UNDER THAT LICENSE SCHEDULE, AND (ii) A MAINTENANCE SERVICES SCHEDULE SHALL BE LIMITED IN THE AGGREGATE TO THE

MAINTENANCE SERVICES FEES PAID BY CLIENT THEREUNDER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRIOR TO THE DATE ON WHICH THE FIRST EVENT OCCURRED ALLEGEDLY GIVING RISE TO DAMAGES. EXCEPT FOR A BREACH BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO BUSINESS INTERRUPTION OR LOST PROFITS OR SAVINGS.

9. TERM AND TERMINATION. This Agreement will commence upon the Effective Date and, unless terminated earlier, will continue until the expiration or termination of the last Schedule still in effect. The term of each license and set of Maintenance Services are set forth in the corresponding Schedule. In addition to any termination rights of the parties set forth in a Schedule, either party may (i) terminate the Agreement for material breach upon thirty (30) days written notice identifying specifically the basis for such notice unless the party receiving the notice cures such breach within the thirty (30) day period; or (ii) upon written notice to terminate if the other party enters bankruptcy proceedings, becomes insolvent, or otherwise becomes unable to meet its obligations under this Agreement. In addition to other available remedies, Accenture may suspend Maintenance Services to Client if the Maintenance Services fees are more than thirty (30) days overdue. In the event this Agreement is terminated, both parties will destroy or return all Information of the other party (except as required for its internal recordkeeping requirements or as permitted by Section 5). Client shall immediately cease all activities authorized hereunder, pay all sums due, and certify in writing destruction or return of all copies of the Software. All provisions of this Agreement related to confidentiality, indemnities, intellectual property ownership and protection, limits of liability, or which are by their nature intended to survive the expiration or termination of this Agreement will survive such expiration or termination.

10. GENERAL

10.1 Assignment. Client may not assign or transfer this Agreement or any of its rights or obligations hereunder, including by operation of law, without the prior written consent of Accenture, and any attempt to do so shall be null and void.

10.2 Compliance with Laws. Each party will retain responsibility for compliance with all laws and regulations applicable to their respective businesses. Each party will comply with applicable export control and sanctions laws with respect to the export or re-export of goods, software and technical data, or the direct product of the same, which includes abiding by all such regulations in respect of all information supplied by or on behalf of the other party. Prior to providing Accenture any goods, software or technical data subject to export controls, Client will provide written notice to Accenture specifying the nature of the controls and any relevant export control classification numbers. Client shall be solely responsible for its use of the Software and documentation and shall ensure that Client complies with any data protection laws applicable to data involved in its business including, without limitation, personal data. Client is responsible for determining if the receipt and use of the Maintenance Services and Software comply with applicable laws, regulations, or industry standards. Client agrees that the Software and documentation are not designed to achieve or contribute to Client's compliance with these or other laws or regulations of any jurisdiction, including the specified territory.

10.3 Data Protection. Accenture and Client shall maintain an information security program including reasonable administrative, technical and physical measures designed to secure and protect the confidentiality of data while in such party's possession against unauthorized, unlawful or accidental access, disclosure, or transfer. The parties agree that Accenture is not required for the purposes of this Agreement to accessor or process any data that identifies or directly relates to natural persons ("Personal Data") and Client agrees not to make any such data available to Accenture. If Client inadvertently provides Accenture with access to Client Personal Data., Accenture shall use reasonable measures to protect such Client Personal Data in its possession until it can be returned or destroyed**.**

10.4 Dispute Resolution. The parties will make good faith efforts to first resolve internally within 30 days any dispute, including over an invoice, relating to this Agreement by escalating it to higher levels of management. If Client withholds an amount more than sixty days Accenture will be permitted to suspend performance until such time as the matter in dispute is resolved. This Agreement shall be governed by and construed in accordance with the laws of the State of New York without regard to its conflict with laws provisions; any litigation relating to this Agreement must be filed in either the state or federal courts of New York.

10.5 Force Majeure. Except for payment obligations, neither party will be liable for any delays or failures to perform due to causes beyond that party's reasonable control (including a force majeure event).

10.6 Notices. Any notice or other communication provided under this Agreement will be in writing, addressed to such party at the address set forth herein, or upon electronic delivery by confirmed means.

10.7 Relationship of the Parties. Nothing in this Agreement is to be construed as creating an agency,

partnership, or joint venture relationship between the parties hereto.

10.8 Audit Rights. Upon request by Accenture, Client shall audit and certify to Accenture that its use of the Software and documentation complies with the Agreement. Accenture reserves the right once every twelve months, upon reasonable prior notice and during normal business hours, to audit usage of the Software and documentation to verify Client's compliance with this Agreement. Accenture may repeat the audit if non-compliance is found.

10.9 Construction of the Agreement. This Agreement, including its Schedules sets forth the entire understanding between two sophisticated business entities with legal counsel as to its subject and supersedes all prior agreements, conditions, warranties, representations, arrangements and communications, whether oral or written, and whether with or by Accenture, any of its affiliates, or any of their employees, officers, directors, agents or shareholders. Each party acknowledges that it entered into this Agreement solely based on the agreements and representations contained herein, and has not relied upon any representations, warranties, promises, or inducements of any kind, whether oral or written, and from any source. If a court of competent jurisdiction finds any term of this Agreement to be invalid, illegal or otherwise unenforceable, such term or provision will not affect the other terms of this Agreement and will be deemed modified to the extent necessary, in the court's opinion, to render such term enforceable while preserving to the fullest extent permissible the intent and agreements of the parties set forth in this Agreement. No waiver or modification of any provision of this Agreement, including any underlying Schedule, will be effective unless it is in writing and signed by the party against which it is sought to be enforced. The delay or failure by either party to exercise or enforce any of its rights under this Agreement is not a waiver of that party's right to later enforce those rights, nor will any single or partial exercise of any such right preclude any other or further exercise of these rights or any other right. There are no third-party beneficiaries to this Agreement. In the event of a conflict between this Agreement and a Schedule, the Schedule controls for purposes of that Schedule only. This Agreement may include one or more Exhibits at the time of execution which shall be listed and considered part of the Agreement.

10.10 Reference Materials. Following execution of a Schedule, Accenture may prepare and distribute (i) a press release announcing the commitment Client has made to the Software; and (ii) a client story discussing business success Client has achieved with the Software. Client will provide Accenture with an executive quote detailing why Client chose the Software which Accenture may include in Software marketing materials (the press release, client story and quote collectively the "Reference Materials"). Content of the Reference Materials will be jointly agreed upon prior to public distribution. Accenture may republish Reference Materials in Accenture Software marketing mediums including, but not limited to Accenture websites, collateral, and newsletters for 1 year following joint approval of such Reference Material content. Client grants to Accenture for the term of this Agreement a limited non-exclusive right to use Client's name and trademarks (collectively, "Client Marks") in promotional materials (including Reference Materials and Accenture's website) to identify Client as an authorized licensee of the Software.

10.11 Federal Use. The Software licensed under this Agreement is "commercial computer software" as that term is defined in 48 CFR 2.101. All U.S. government end users acquire the Software with only those rights set forth in this Agreement, in accordance with 48 CFR 12.212(b) and/ or 48 CFR 227.7202-1(a) and 48 CFR 227.7202-4, as applicable.

10.12 Other Services. Accenture may provide training, on-site support, implementation, integration, configuration, customization and other services not explicitly set forth in this Agreement provided the parties have executed a separate mutually agreed professional services agreement which shall exclusively govern such services.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of [INSERT DATE] ("Effective Date").

ACCENTURE
< Local Accenture entity>
< Local Accenture address>

By:_____

Name/Title:_____

Date:_____

CLIENT
<Client legal name>
< Client address>

By:_____

Name/Title:_____

Date:_____

APP SAAS AGREEMENT

ACCENTURE SOFTWARE-AS- A-SERVICE AGREEMENT

[NAME OF LOCAL ACCENTURE ENTITY] ("Accenture") will provide the Software-as-a-Service to _____ ("Client") as specified in separately signed service orders ("Service Orders") under the following terms and conditions (collectively the "Agreement").

1 **CLIENT'S RIGHTS AND OBLIGATIONS**

1.1 Subject to Client's payment of the fees specified in and compliance with the terms and conditions of this Agreement and the relevant Service Order, Accenture hereby grants to Client a non-exclusive, non-transferable right during the term of the applicable Service Order to permit its Authorized Users to access and use the SaaS Services for the Permitted Purpose only.

1.2 Client agrees that, unless explicitly authorized pursuant to the Permitted Purpose, it shall not license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit the SaaS Services by making them available for access or use by any third party (except Authorized Users), including by means of operating a service bureau, outsourcing or time-sharing service.

1.3 Client shall be solely responsible for (i) determining the suitability of the SaaS Services for its purposes and those of its Authorized Users and (ii) ensuring that Client's or its Authorized Users' use of the SaaS Services shall not exceed any restrictions contained in this Agreement or the applicable Service Order. In particular, the Client shall ensure that (i) if applicable, the maximum number of Authorized Users that it authorises to access and use the SaaS Services shall not exceed the number of user subscriptions it has purchased from time to time as set out in a Service Order, and (ii) it will not allow or suffer any user account to be used by more than one individual Authorized User unless it has been reassigned in its entirety to another individual Authorized User, in which case the prior Authorized User shall no longer have any right to access or use the SaaS Services.

1.4 Client is responsible for all use of the SaaS Services by those who have access to them through Client's credential, and for ensuring that its Authorized Users do not circumvent or disclose any usernames, passwords or other access credentials or authentication details, or interfere with or disrupt any other security control of the SaaS Services.

1.5 Client shall maintain commercially reasonable security standards for its and its Authorized Users' use of the SaaS Services. Specifically, Client will use good industry practice virus protection software, and other customary procedures to screen any Client Content to avoid introducing any Virus or other malicious files or other harmful code that could disrupt the proper operation of the systems used in the provision of the SaaS Services. Client also agrees that it shall use all reasonable endeavors to ensure that its Authorized Users do not upload or distribute files that contain Viruses, or do anything else to disrupt or attempt to disrupt, the systems and networks used for the provision of the SaaS Services. If Client learns or suspects that its Authorized Users have introduced a Virus, Client will notify Accenture and cooperate in mitigating the effects of such Virus.

1.6 Client shall be solely responsible for the acts and omissions of its Authorized Users as if they were the acts and omissions of Client, and for ensuring that anyone who uses the SaaS Services does so in accordance with the terms and conditions of this Agreement and the applicable Service Order. In particular, the Client agrees that it shall not, and that it shall ensure that its Authorized Users do not: (i) access or use the SaaS Services to host or transmit any content, data or information that is illegal or which infringes any third party's rights, such as intellectual property rights or right of privacy, or which otherwise violates any applicable laws; (ii) copy, translate, make derivative works, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code or underlying ideas or algorithms embodied in the software applications or other systems used for the provision of the SaaS Services (including the IaaS), unless expressly permitted under any applicable laws, or remove any titles or trademarks, copyrights or restricted rights notices in the systems, software and other materials used in the provision of SaaS Services; or (iii) access or use the SaaS Services for the purpose of building competitive products or services by copying its features or user interface or by allowing a direct competitor of Accenture to access or use the SaaS Services.

1.7 Client will notify Accenture immediately if it becomes aware of any breach or threatened breach of the terms of this Section 1, or of any breach or threatened breach of security including any attempt by a third party to gain unauthorized access to the systems used for the provision of the SaaS Services.

1.8 Client acknowledges and agrees that it is responsible for obtaining and maintaining all hardware, software, communications equipment and network connections necessary to access and use the SaaS Services, and for

paying any applicable third-party fees and charges incurred while accessing and using the SaaS Services.

2 **ACCENTURE'S RIGHTS AND OBLIGATIONS**

2.1 Accenture shall provide the SaaS Services in accordance with an executed Service Order.

2.2 In providing the SaaS Services Accenture will use reasonable and appropriate technical and organizational security measures intended to safeguard Client Content against accidental, unauthorized or unlawful access, loss, damage or destruction.

2.3 Accenture may need to apply updates or make changes to the SaaS Services that it is providing pursuant to any Service Order, provided always that Accenture shall not be entitled to apply such updates or other changes in a manner that would make the SaaS Services materially non-conforming with the applicable service descriptions, or otherwise materially diminish the scope or the quality of the service provided, unless such changes are necessary for Accenture to comply with any applicable laws. Accenture will notify the Client reasonably in advance of any planned changes to the SaaS Services that have any material impact on Client's access to or use thereof.

2.4 Client acknowledges and agrees that Accenture shall be permitted to monitor the Client's and its Authorized Users' access and usage of the SaaS Services limited solely for the purposes of verifying Client's compliance with the terms of this Agreement and the applicable Service Order.

2.5 Client hereby acknowledges, accepts and agrees that Accenture may have to suspend Client's and/or its Authorized Users' right to access or use all or any portion of the SaaS Services, or remove any relevant Client Content as described below: (i) where such access or use, or any Client Content (x) poses a security risk to or may otherwise adversely impact the SaaS Services or (y) infringes or otherwise violates the rights or other interests of a third party, entails illegal or otherwise prohibited content or activities, or otherwise subjects Accenture to a potential liability; (ii) where Client has materially breached its obligations under Section 4 and, within 10 business days of Accenture's written notice thereof, fails to remedy such breach; or (iii) where Accenture is required to do so under any applicable laws, or any court's or governmental body's order.

2.6 When allowed under the applicable laws and if otherwise reasonable under the circumstances (as determined by Accenture in its discretion), Accenture shall provide Client with a written notice prior to such suspension, and an opportunity to take steps to avoid any such suspension. Any suspension of Client's or its Authorized Users' right to access or use the SaaS Services shall not release the Client from its obligations under this Agreement and any Service Order, including any obligation of paying the fees. Accenture's suspension right is in addition to Accenture's right to terminate this Agreement or any Service Order pursuant to Section 9.

3 **CLIENT CONTENT**

3.1 Client (and Client's licensors, where applicable) own all right, title and interest in and to the Client Content.

3.2 Client has obtained, and during the Term will obtain, all Consents required under applicable law prior to Client Content being entered into or processed by the SaaS Services. In particular, Client has collected and shall maintain and handle all Personal Information contained in Client Content in compliance with all applicable data privacy and protection laws, rules and regulations.

3.3 Client authorizes Accenture to process its Personal Information in accordance with Client's written instructions as set out in this Agreement and the applicable Service Order. Client has satisfied itself that Accenture and any applicable Cloud Vendor have in place appropriate technical and organizational measures to protect Client Content (including Personal Information) processed on behalf of Client from unauthorized use or access, accidental loss, damage, destruction, theft or disclosure. If the SaaS Services involve the processing of Client Personal Information within the scope of the EU General Data Protection Regulation ("GDPR"), then the terms of Exhibit B (GDPR Exhibit) shall also apply. If the SaaS Services involve the processing of Protected Health Information (as defined in 45 CFR 160.103, the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA)), a Business Associate Agreement (BAA) or its equivalent shall be executed and attached as an Exhibit to the applicable Service Order.

3.4 Client grants to Accenture the nonexclusive right to host, store, process, modify and transfer the Client Content for the purposes of Accenture's provision of, and Client's use of, the SaaS Services as set forth in this Agreement, and Accenture's improvement of the SaaS Services incidental to such use. Accenture agrees to destroy any Client Content in accordance with Section 9.7 of this Agreement. Accenture may: (i) use usage patterns, trends, statistics, and other data derived from use of the SaaS Services (but not Client Content itself) for purposes of developing or improving the SaaS Services and other Accenture products and services; and (ii) provide information to the Cloud Vendor regarding Client's use of the IaaS, subject to the Cloud Vendor's obligations of confidentiality, for Cloud Vendor's use to improve its cloud infrastructure services.

3.5 Client shall have the ability to access its Client Content hosted in the SaaS Services at any time during the term

of the applicable Service Order. Client may export and retrieve its Client Content during such Service Order term, subject to any technical limitations in the SaaS Services or Client's and its Authorized Users' hardware and software, including factors such as (i) the size of Client's instance of the SaaS Services; and (ii) the frequency and/or timing of the export and retrieval.

4 **FEES, PAYMENTS AND TAXES.** Accenture shall invoice and Client shall pay the fees specified in the applicable Service Order. Fees are stated exclusive of all applicable duties, tariffs, and taxes. Unless otherwise specified in a Service Order, fees will be due and payable within thirty (30) days of Accenture's invoice. Should any invoice (excluding disputed amounts) become overdue by more than thirty (30) days, interest will be charged at a rate of 1% per month or the highest rate allowed by law, whichever is less from the original invoice due date, until the overdue balance is settled. Any taxes arising out of this Agreement other than those on Accenture's net income will be Client's responsibility. Accenture will pay any taxes remitted to it by Client to the applicable taxing authority when due. The Parties agree to cooperate to help enable each party to accurately determine and reduce its own tax liability and to minimize any potential liability to the extent legally permissible. All amounts payable under this Agreement will be made without set-off or counterclaim, and without any deduction or withholding.

5 **ACCENTURE'S INTELLECTUAL PROPERTY RIGHTS.** Accenture and its licensors, where applicable, own all right, title and interest, including all Intellectual Property Rights, in and to the systems, software and other content and materials used in the provision of the SaaS Services, and to any suggestions, enhancement requests, feedback, or recommendations provided by Client or any other party relating thereto. Client may only use the SaaS Services and Accenture's Intellectual Property Rights relating thereto as expressly permitted herein. The Accenture name, the Accenture logo, and the product names associated with the SaaS Services are trademarks of Accenture or third parties, and no right or license is granted to Client to use them.

6 **WARRANTIES AND EXCLUSIONS**

6.1 Accenture warrants that the SaaS Services provided to Client pursuant to this Agreement will comply in all material respects with the Documentation identified in the applicable Service Order. This warranty shall not apply where: (i) the Client's or any Authorized User's access or use of the SaaS Services is not in compliance with this Agreement or with Accenture's instructions; (ii) modification or alteration of the SaaS Services or any systems, software or other content or materials embodied therein is made by any Party other than Accenture; or (iii) the SaaS Services are being provided free of charge, or as a trial, pre-release or as a beta release.

6.2 Client shall provide Accenture with prompt written notice of any non-conformity of the SaaS Services specified in Section 6.1, sufficiently describing such non-conformity, no later than within thirty (30) days of the appearance or Client's discovery of such non-conformity.

6.3 In such event, Accenture will use commercially reasonable efforts to correct any such non-conformity. In the event Accenture is unable to correct such non-conformity by exercising commercially reasonable efforts for a reasonable period, either Party may terminate the relevant Service Order concerning the non-conforming SaaS Service(s) on written notice to the other Party in which case as Client's sole and exclusive remedy, Accenture will provide a pro-rated refund of any pre-paid fees for periods after the effective date of termination.

6.4 Accenture shall provide the SaaS Services by using good industry practice virus protection software to detect and mitigate Viruses in the SaaS Services (separate from the Client Content) that could disrupt the proper operation of the systems used in the provision of the SaaS Services.

6.5 **Disclaimer.** THE WARRANTIES SET FORTH IN THIS SECTION 6 ARE THE ONLY WARRANTIES CONCERNING THE SAAS SERVICES OR THIS AGREEMENT MADE BY ACCENTURE, AND ARE MADE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, CONDITIONS AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY THAT THE SAAS SERVICES WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING CLIENT CONTENT OR THIRD PARTY COMPONENTS OR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED, AND 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. EACH PARTY, ITS AFFILIATES AND ITS LICENSORS DISCLAIM ALL, AND THE OTHER PARTY AGREES THAT IT IS NOT ENTITLED TO ANY EQUITABLE OR IMPLIED INDEMNITIES. THESE DISCLAIMERS SHALL ONLY APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW.

7 **INDEMNITY**

7.1 Accenture will defend Client, its parents, subsidiaries, affiliates, successors, and their directors, officers, employees, agents and representatives (its "Indemnified Parties") from and against any and all third party claims,

demands, lawsuits, judgments, fines, and penalties (including interest thereon and court costs) caused by a claim brought against Client by any third party (that is not an Indemnified Party) that Client's use of the SaaS Services, in accordance with the terms and conditions of the Agreement and the applicable Service Order, constitutes a direct infringement of a patent issued in the United States as of the Effective Date, copyright, or trade secret of any third party.

7.2 Accenture will have no obligations or liability under Section 7.1 for any claims to the extent arising from:

7.2.1 Client Content;

7.2.2 Client's or any Authorized User's use of the SaaS Services after Accenture has notified Client to discontinue such use and Client have been afforded a reasonable opportunity to discontinue such use;

7.2.3 any unauthorized modification or unauthorized use of the SaaS Services where infringement or misappropriation would not have occurred but for such unauthorized modification or unauthorized use;

7.2.4 any use of the SaaS Services, or any other act, by Client or an Authorized User, that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for the breach;

7.2.5 any claim of wilful infringement adjudicated against anyone other than Accenture and its affiliates or Cloud Vendor;

7.2.6 any combination(s) of the SaaS Services with any other product, service, software, content, data or method not supplied by Accenture; or

7.2.7 a free (no fee) or trial license of the SaaS Services.

7.3 If any portion of the SaaS Services are, or in Accenture's opinion are likely to be, held to be infringing, Accenture may choose (at its election and expense) to: (a) procure the rights to use the item alleged to be infringing; (b) replace the alleged infringing portion with a non-infringing equivalent; or (c) modify the alleged infringing portion to make it non-infringing while still providing substantially the same level of functionality. If Accenture determines the actions from Section 7.3 (a) to (c) are not commercially reasonable, Accenture may immediately terminate Client's access to the SaaS Services.

7.4 Client shall defend (at its sole expense) Accenture and its Indemnified Parties and licensors from and against any and all third party claims, demands, lawsuits, judgments, fines, and penalties (including interest thereon and court costs) caused by a claim brought against Accenture by any third party (that is not an Indemnified Party or licensor) arising from or related to (a) any use of SaaS Services by Client or its Authorized Users in violation of any applicable law or regulation; or (b) any allegation that the Client Content violates, infringes or misappropriates the rights of a third party; or (c) Client's or its Authorized Users' use of the SaaS Services or other act in violation of this Agreement or the relevant Service Order. The foregoing shall apply regardless of whether such damage is caused by the conduct of Client and/or its Authorized Users or by the conduct of a third party using Client's or an Authorized User's access credentials where Client has negligently made the credentials available or chosen credentials that are easy to hack into.

7.5 Client will have no obligations of liability under Section 7.4 for any claims arising from:

7.5.1 Client Content after Client has notified Accenture to delete the Client Content from the SaaS and Accenture has been afforded a reasonable opportunity to do so; or

7.5.2 any unauthorized access or use of the Client Content by Accenture that is in breach of this Agreement, where the infringement or misappropriation would not have occurred but for such breach.

7.6 In connection with any third party claims pursuant to Section 7.1 or 7.4, the indemnified Party (on behalf of itself or any Indemnified Party) will (a) give the indemnifying Party prompt written notice of the claim; (b) reasonably cooperate with the indemnifying Party (at the indemnifying Party's expense) in connection with the defense and settlement of such claim, and (c) grant the indemnifying Party sole control of the defense and settlement of the claim, except that the indemnifying Party may not consent to the entry of any judgment or enter into any settlement with respect to the claim without the indemnified Party's prior written consent unless the settlement or judgment is purely financial, is paid entirely by the indemnifying Party, is confidential, does not require the indemnified Party to admit to any fault or wrongdoing, and fully releases the indemnified Party from any and all further claims or causes of action relating to the subject matter of the claim. The non-controlling Party may, at its expense, participate in the defense and settlement of the claim with counsel of its own choosing. If the indemnifying Party fails to assume control within 30 days of written notice of the claim, the indemnified Party may assume control of the defense of the claim

7.7 **Exclusive Remedy**. SECTION 7.1 CONSTITUTES CLIENT'S SOLE AND EXCLUSIVE REMEDY AND ACCENTURE'S (AND ITS AFFILIATES') ENTIRE OBLIGATION TO CLIENT WITH RESPECT TO ANY CLAIM THAT THE SAAS SERVICES INFRINGE OR MISAPPROPRIATE THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

8 **LIMITATION OF LIABILITY**

8.1 EXCEPT FOR (I) BREACH OF ITS OBLIGATIONS UNDER SECTION 4 OR 7, (II) A BREACH OF ACCENTURE'S INTELLECTUAL PROPERTY RIGHTS UNDER SECTION 5, OR (III) DAMAGES RESULTING FROM DEATH OR BODILY INJURY ARISING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OR FROM FRAUD OR FRAUDULENT MISREPRESENTATION, UNDER NO CIRCUMSTANCES AND REGARDLESS OF THE NATURE OF ANY CLAIM SHALL EITHER PARTY (OR THEIR RESPECTIVE AFFILIATES OR ACCENTURE'S LICENSORS) BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY UNDER THIS AGREEMENT FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID UNDER A SERVICE ORDER FOR THE APPLICABLE SAAS SERVICES IN THE TWELVE (12) MONTH PERIOD PRECEDING THE DATE OF THE INCIDENT GIVING RISE TO LIABILITY.

8.2 TO THE EXTENT PERMITTED BY LAW, EXCEPT FOR A BREACH OF ACCENTURE'S INTELLECTUAL PROPERTY RIGHTS UNDER SECTION 5, NEITHER PARTY NOR ANY OF EITHER PARTY'S RESPECTIVE AFFILIATES WILL BE LIABLE TO THE OTHER PARTY UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES; BUSINESS INTERRUPTION, LOSS OF PROFITS OR SAVINGS, REVENUES, OR GOODWILL; LOSS OR CORRUPTION OF DATA; UNAVAILABILITY OF ANY OR ALL OF THE SAAS SERVICES; INVESTMENTS, EXPENDITURES OR COMMITMENTS RELATED TO USE OF OR ACCESS TO THE SAAS SERVICES; COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; UNAUTHORIZED ACCESS TO, COMPROMISE, ALTERATION OR LOSS OF CLIENT CONTENT OR BUSINESS INFORMATION; OR COST OF REPLACEMENT OR RESTORATION OF ANY LOST OR ALTERED CLIENT CONTENT.

8.3 The Parties acknowledge that the limitations on liability set out in this Section 8 are essential terms of this Agreement, and the Parties would not have entered this Agreement without them.

9 **TERM AND TERMINATION**

9.1 The term of this Agreement will commence on the Effective Date and will continue until terminated by either Party pursuant to this Section 9. The term of any Service Order shall be agreed in the Service Order itself, and the terms and conditions of this Agreement shall survive and remain in force to govern any Service Order the term of which exceeds any termination of this Agreement.

9.2 Either Party may terminate this Agreement (but not a Service Order) for convenience upon sixty (60) days written notice to the other Party. For the avoidance of doubt, either Party may only terminate a Service Order in accordance with the terms of the Service Order or as expressly provided for in this Agreement.

9.3 Either Party may terminate this Agreement and/or any Service Order upon written notice if the other Party ceases its business operations or becomes subject to insolvency proceedings or any similar or equivalent process in any jurisdiction, and the proceedings are not dismissed within ninety (90) days, or otherwise becomes generally unable to meet its obligations under this Agreement and/or the Service Order.

9.4 In addition to any other remedies that a Party may have at Law, in equity, or under this Agreement, a Party may terminate this Agreement and/or any Service Order upon thirty (30) days' advance written notice to the other Party if the other Party commits any material breach of this Agreement and/or any Service Order and fails to cure such default (if curable) within the thirty (30) day period, including if there has been any such act or omission by Client or any Authorized User that has given Accenture the right to suspend the provision of SaaS Services in accordance with Section 2.6.

9.5 Accenture may also terminate this Agreement and/or any Service Order without liability upon thirty (30) days' notice to Client or any Authorized User: (i) in the event where an underlying contract between Accenture and the Cloud Vendor concerning the provision of the IaaS terminates, or (ii) if termination of the Agreement and/or any Service Order is necessary to comply with applicable law or binding requests of governmental entities.

9.6 Upon the effective date of expiration or termination of a Service Order, Client shall cease Client's and its Authorized Users' access to and use of the SaaS Services.

9.7 If agreed in the applicable Service Order, Accenture will provide Client with the ability to retrieve Client Content after the expiration or termination of such Service Order for a limited period of time, in which case Client will cover the costs of the data storage unless otherwise agreed in the Service Order. Otherwise, Accenture will destroy, procure the destruction of, or otherwise dispose of any Client Content in its possession or in possession of a Cloud Vendor (including any data back-ups) upon expiration or termination of the applicable Service Order.

9.8 If so mutually agreed in the Service Order, Accenture shall provide to Client reasonable cooperation and assistance to facilitate the orderly wind down of the usage of the SaaS Services and/or to assist Client to transition to another provider. Client will pay Accenture for such assistance at Accenture's then-current time and materials rates for the applicable services or as otherwise mutually agreed by Client and Accenture. If the termination results from a breach of this Agreement by

Client, Accenture may invoice Client in advance for all transition assistance services and, if so invoiced, Client will pay in advance.

10 **CONFIDENTIALITY**

10.1 Each Party agrees that it will use the other Party's Confidential Information only to the extent reasonably necessary for purposes of this Agreement or a Service Order, and to protect such Confidential Information in the same manner that it protects its own similar confidential information, but in no event using less than a reasonable standard of care. Access to the Confidential Information will be restricted to Accenture and Client personnel (including such personnel employed by their affiliates) and subcontractors with a need to use such Confidential Information pursuant to the parties' rights and obligations under this Agreement, provided such parties are bound by substantially similar obligations of confidentiality [and are not listed as a competitor in the applicable Schedule]. Accenture may retain and use Confidential Information relevant to its business purposes (including to provide or enhance its services) so long as its use of such Information is in an aggregated and anonymized or pseudonymized manner. Nothing in this Agreement will prohibit or limit either party's use of Confidential Information (i) previously known to it without an obligation not to disclose such information, (ii) independently developed by or for it without use of Confidential Information, (iii) acquired by it from a third party which was not, to the receiver's knowledge, under an obligation not to disclose such information, or (iv) which is or becomes publicly available through no breach of this Agreement. Client shall not disclose the terms and conditions of this Agreement or the pricing contained herein to any third party unless otherwise agreed by the Parties.

11 **ADDITIONAL TERMS**

11.1 **Compliance with Laws.** Accenture will comply with all laws applicable to it and its business in providing the SaaS Services, and Client will comply with all laws applicable to it and its business in providing the Client Content and in using the SaaS Services and ensure that the way that it and its Authorized Users access and use the SaaS Services complies with any applicable laws. Each Party will comply with relevant data privacy laws to the extent applicable to such Party in its role with respect to the processing of Client Personal Information under this Agreement. Each Party will comply with all export control and economic sanctions laws applicable to its performance under this Agreement. Client agrees that Client will and will ensure that Authorized Users do not use the SaaS Services in or in relation to any activities involving a country subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria or the Crimea region of Ukraine), or involving a Party in violation of such applicable trade control laws, or that require government authorization, without first obtaining the informed consent of Accenture and the required authorization. For the avoidance of doubt, Client shall not grant access to the SaaS Services to any individual, entity or organization which is subject to trade sanctions or embargos by the United States or any applicable jurisdiction, including any individual, entity or organization which is listed on the OFAC Specially Designated Nationals List from time to time.

11.2 **Notices**. Unless expressly stated otherwise in this Agreement, any notice or other communication provided under this Agreement will be in writing, addressed to such party at the address set forth herein, or upon electronic delivery by confirmed means.

11.3 **Disputes, Governing Law and Jurisdiction**. The Parties will make good faith efforts to first resolve internally within 30 days any dispute, including over an invoice, in connection with this Agreement by escalating it to higher levels of management. If Client withholds an amount more than sixty days Accenture will be permitted to suspend performance until such time as the matter in dispute is resolved. The laws of the State of Illinois and federal laws of the United States will govern the construction, validity and operation of this Agreement and the performance of all obligations hereunder without regard for Illinois' choice of law provisions. The courts of Chicago, Illinois shall have exclusive jurisdiction in relation to any dispute or matter arising under or in connection with this Agreement.

11.4 **Force Majeure**. Except for payment obligations, neither party will be liable for any delays or failures to perform due to causes beyond that party's reasonable control (including a force majeure event).

11.5 **Survival**. The provisions of Sections 5, 6.5, 7, 8, 9, 10, and 11, and any other Sections which by their nature are intended to survive, will survive the termination or expiration of this Agreement.

11.6 **Assignment**. Client may not assign this Agreement or delegate or sublicense any of Client's rights or obligations hereunder, including by operation of law, without the prior written consent of Accenture and any attempt to do so in violation of this provision will be null and void.

11.7 **Variation**. Except as otherwise expressly provided to the contrary in this Agreement, this Agreement may only be changed, modified or expanded by a writing signed by both Parties.

11.8 **Construction of the Agreement**. Each executed Service Order constitutes a separate and binding agreement, incorporating the terms and conditions of this

Agreement. This Agreement, including its Service Orders, sets forth the entire understanding between two sophisticated business entities with legal counsel as to its subject and supersedes all prior agreements, conditions, warranties, representations, arrangements and communications, whether oral or written, and whether with or by Accenture, any of its affiliates, or any of their employees, officers, directors, agents or shareholders. Each party acknowledges that it entered into this Agreement solely based on the agreements and representations contained herein, and has not relied upon any representations, warranties, promises, or inducements of any kind, whether oral or written, and from any source. If a court of competent jurisdiction finds any term of this Agreement to be invalid, illegal or otherwise unenforceable, such term or provision will not affect the other terms of this Agreement and will be deemed modified to the extent necessary, in the court's opinion, to render such term enforceable while preserving to the fullest extent permissible the intent and agreements of the parties set forth in this Agreement. No waiver or modification of any provision of this Agreement, including any underlying Schedule, will be effective unless it is in writing and signed by the party against which it is sought to be enforced. The delay or failure by either party to exercise or enforce any of its rights under this Agreement is not a waiver of that party's right to later enforce those rights, nor will any single or partial exercise of any such right preclude any other or further exercise of these rights or any other right. There are no third-party beneficiaries to this Agreement except for Accenture's licensors. The capitalized terms as used in this Agreement have the meanings set out in the body of this Agreement or in Exhibit A (Definitions). If there is a conflict between the terms and conditions of this Agreement and those of any Service Order, then the following order of precedence shall apply: (i) the Service Order; (ii) any schedules or attachments to the Service Order and any other documents incorporated thereto by reference; (iii) the terms and conditions of this Agreement; and (iv) any exhibits to this Agreement. Except as a Service Order may otherwise expressly provide, each Service Order will be a complete statement of its subject matter and will supplement and modify the terms and conditions of this Agreement for purposes of that Service Order only.

11.9 **Relationship of the Parties**. Nothing in this Agreement is to be construed as creating an agency, partnership, or joint venture relationship between the parties hereto.

11.10 **Audit Rights.** Upon request by Accenture, Client shall audit and certify to Accenture that its use of the SaaS Services complies with the Agreement. Accenture reserves the right once every twelve months, upon reasonable prior notice and during normal business hours, to audit usage of the SaaS Services to verify Client's compliance with this Agreement. Accenture may repeat the audit if non-compliance is found.

11.11 **Counterparts.** This Agreement may be executed in any number of counterparts and executed by facsimile or by other electronic communication as agreed upon by the Parties, such execution to be considered an original for all purposes, and all of which together will constitute one and the same instrument, notwithstanding that the Parties may not both be signatories to the original or same counterpart.

11.12 **Reference Materials.** Following execution of a Service Order, Accenture may prepare and distribute Reference Materials. Content of the Reference Materials will be jointly agreed upon prior to public distribution. Accenture may republish Reference Materials in Accenture marketing mediums including, but not limited to Accenture websites, collateral, and newsletters for 1 year following joint approval of such Reference Material content. Client grants to Accenture for the term of this Agreement a limited non-exclusive right to use Client's name and trademarks in promotional materials (including Reference Materials and Accenture's website) to identify Client as an authorized user of the SaaS Services.

11.13 **Business Contact Information**. Each party consents to the other party using its Business Contact Information for contract management, payment processing, service offering, and business development purposes related to this Agreement and such other purposes as set out in the using party's global data privacy policy (copies of which shall be made available upon request). For such purposes, and notwithstanding anything else set forth in this Agreement with respect to Client Personal Information in general, each party shall be considered a data controller with respect to the other party's Business Contact Information and shall be entitled to transfer such information to any country where such party's global organization operates.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of [INSERT DATE] ("Effective Date").

ACCENTURE:	**Client: _____**
BY: _____	BY: _____
PRINTED NAME: _____	PRINTED NAME: _____
TITLE: _____	TITLE: _____
DATE: _____	DATE: _____

EXHIBIT A
DEFINITIONS

"**Authorized User**" means any individual or entity that, directly or indirectly through another Authorized User, accesses or uses the SaaS Services;

"**Business Contact Information**" means the names, mailing addresses, email addresses, and phone numbers of a party's personnel, officers and directors and, with respect to Client, such information regarding Client's vendors and customers that Accenture may have access to in maintaining the parties' business relationship.

"**Cloud Vendor**" means the relevant cloud service provider, providing the IaaS;

"**Client Content**" means any content, materials, data and information, including Personal Information that Client or its Authorized Users enter into the SaaS Services or is otherwise uploaded by or on behalf of Client to the SaaS Services. Client Content shall not include any component of the SaaS Services or material or data provided by or on behalf of Accenture or its licensors.

Client Personal Information" means Personal Information provided to Accenture by or on behalf of Client in connection with this Agreement, in the form of Client Content;

"**Confidential Information**" means the SaaS Service and any information that relates to a party's (or to Cloud Vendor's) past, present, or future research, development, business activities, products, services, and technical knowledge, which is identified by the discloser as confidential or that would be understood to be confidential by a reasonable person under the circumstances. For the purposes of this Agreement, the term "Confidential Information" does not include Client Content;

"Consent" means (1) all consents, permissions, notices and authorizations necessary for Accenture to provide the SaaS Services, including from Client employees or third parties; (2) valid consents from or notices to applicable individuals whose data is processed by the SaaS Service); and (3) required authorizations from regulatory authorities, employee representative bodies or other applicable third parties;

"**Effective Date**" means the date first written above;

"Documentation" means _____ ;

"**IaaS**" means the infrastructure-as-a-service provided by a Cloud Vendor on which the SaaS Services are hosted or is otherwise utilized in the provision of the SaaS Services by Accenture;

"**Intellectual Property Rights**" means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights, derivatives thereof, and forms of protection of a similar nature;

"Permitted Purpose" has the meaning given to such term in the applicable Service Order. If the applicable Service Order does not define Permitted Purpose, it will mean Client's internal business purposes;

"**Personal Information**" means data which names or identifies a natural person including, without limitation: (a) data that is explicitly defined as a regulated category of data under data privacy laws applicable to Client; (b) non-public personal data, such as national identification number, passport number, social security number, driver's license number; (c) health or medical information, such as insurance information, medical prognosis, diagnosis information or genetic information; (d) financial information; and/or (e) sensitive personal data, such as race, religion, marital status, disability, or sexuality;

"Reference Materials" means an Accenture press release announcing the commitment Client has made to the SaaS Services and a client story discussing business success Client has achieved with the SaaS Services, including without limitation an executive quote provided by Client detailing why Client chose the SaaS Services.

"**SaaS Services"** means the hosted solution made available by Accenture for Client's access and use on a subscription basis, as detailed in the applicable Service Order. The term "SaaS Services" includes any modifications, enhancements, additions, extensions, translations and derivative works thereof, and any configuration and related services. The SaaS Services do not include Client Content or any Client-provided third party software;

"**Service Order"** means the documents referenced in Section 1.2, and its Schedules, and any other documents incorporated by reference herein, together with any amendments thereto duly executed by the Parties;

"**Virus**" means any item, software, device or code which is intended by any person to, or which is likely to, or which may (a) impair the operation of any software or computer systems; (b) cause loss of, or corruption or damage to any software or computer systems or data; (c) prevent access to or allow unauthorised access to any software or computer system or data; or (d) damage the reputation of the Client and / or Accenture, including any computer virus, Trojan horse, worm, software bomb, authorization key, license control utility or software lock.

EXHIBIT B
GDPR TERMS

This **Exhibit B** - **GDPR TERMS** ("**Exhibit B**") describes the responsibilities of the Parties with respect to any Client Personal Information processed by Accenture on Client's behalf in connection with the SaaS Services provided under any Service Order where such processing occurs within the scope of the EU General Data Protection Regulation ("**GDPR**"). This Exhibit B is subject to the terms and conditions of the **Accenture *Software-as-a-Service* Agreement** ("**Agreement**") dated _____ between _____ ("**Client**") and [Accenture, LLP] ("**Accenture**") and will be deemed part of the Agreement. Terms not defined below shall have the meaning set forth in the Agreement. If there is a conflict between the Agreement and this Exhibit B, this Exhibit B shall prevail.

Except as otherwise expressly stated in a Service Order, Client shall be the controller of Client Personal Information, and Accenture shall be the processor of such data and each Party shall comply with the relevant data privacy laws to the extent applicable to such Party in its respective role. The Parties hereby acknowledge and agree to the following with respect to the processing of any Client Personal Information under this Agreement:

(a) The applicable Service Order shall set out (i) the subject matter and duration of the processing; (ii) the nature and purpose of the processing; and (iii) the type of Personal Information and categories of data subjects involved.

(b) Accenture will process the Client Personal Information only in accordance with Client's documented processing instructions as set forth in this Agreement and the applicable Service Order, unless otherwise required by law.

(c) All Accenture personnel, including subcontractors, authorized to process the Client Personal Information shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.

(d) Each Party shall implement appropriate technical and organizational security measures to safeguard Client Personal Information from unauthorized processing or accidental loss or damage, as further described in [Exhibit XX of the Agreement] and the applicable Service Order. Client acknowledges and agrees that, taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Information, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in [Exhibit XX of the Agreement] and the applicable Service Order provide a level of security appropriate to the risk in respect of the processing of the Client Personal Information.

(e) Client specifically authorizes the engagement of Accenture's affiliates as subprocessors and generally authorizes the engagement of other third parties as subprocessors as identified in the applicable Service Order. Accenture shall contractually require any such subprocessors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder to the extent applicable to the subprocessors' subcontracted services. Accenture shall remain fully liable for the performance of the subprocessors. Accenture shall provide Client with written notice of any intended changes to the authorized subprocessors and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes. If Client's objection is based on anything other than the proposed subprocessor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the Parties shall be resolved via the contract dispute resolution procedure.

(f) Taking into account the nature of the processing, Accenture shall provide assistance to Client as reasonably requested in responding to requests by data subjects to exercise the rights set out in Chapter III of the GDPR, including rights of access, rectification, erasure, portability, and the right to restrict or object to certain processing. Client shall be responsible for the reasonable costs of such assistance.

(g) Taking into account the nature of the processing and the information available to Accenture, Accenture shall provide reasonable assistance to Client with respect to: (i) Client's implementation of appropriate security measures; (ii) Client's obligation to notify regulators and data subjects of a breach with respect to Client Personal Information as required by GDPR; (iii) Client's obligation to conduct data protection impact assessments with respect to the processing as required by GDPR; and (iv) Client's obligations to consult with regulators as required by GDPR. Client shall be responsible for the reasonable costs of such assistance.

(h) Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in this Exhibit B and, and Accenture shall submit to audits and inspections by Client (or Client directed third parties) in accordance with a mutually agreed process designed

to avoid disruption of the SaaS Services and protect the confidential information of Accenture and its other clients. With regard to this subsection (h), Accenture shall inform Client if, in Accenture's opinion, any Client instruction infringes any applicable data privacy law.

(i) Client acknowledges that Accenture's Cloud Vendors use external, independent auditors to audit and verify the adequacy of their security measures, including the security of their physical data centers, and generate an audit report, available annually ("Report"). The Reports are the Cloud Vendors' Confidential Information and will be available to Client, at Client's request, subject to Client executing the applicable Cloud Vendor's standard non-disclosure agreement**.** Client agrees to exercise any right to conduct an audit or inspection of a Cloud Vendor, including under the EU Model Clauses (defined in Section (k)) if applicable, by instructing Accenture to obtain the relevant Cloud Vendor's Report, as described in this Section. Client may change this instruction at any time upon written notice to Accenture, provided if the Cloud Vendor declines to submit to an audit or inspection requested by Client, Accenture will not be in breach of this Agreement or the applicable Service Order, but Client is entitled to terminate the applicable Service Order to which such request relates upon 30 days' notice to Accenture. If the EU Model Clauses apply, nothing in this Section modifies the EU Model Clauses, and nothing in this Section affects any supervisory authority's or data subject's rights under the EU Model Clauses.

(j) Upon expiration or termination of the SaaS Services, Accenture shall return or destroy any Client Personal Information in accordance with the terms and timelines agreed in the applicable Service Order, unless otherwise required by applicable laws. Unless otherwise agreed, Accenture will comply with any Client deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.

(k) The Parties shall rely on the Standard Contractual Clauses for the Transfers of Personal Data to Processors Established in Third Countries, dated 5 February 2010 (2010/87/EU) as amended from time to time (the "EU Model Clauses") to protect Client Personal Information being transferred from a country within the European Economic Area to a country outside the European Union not recognized by the European Commission as providing an adequate level of protection for Personal Information. Where the transfer relies on the EU Model Clauses, the Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such EU Model Clauses with the relevant Accenture entity or a third-party entity, acting as a data importer.

(l) Client is responsible for reviewing the terms of this Exhibit B and making an independent determination as to whether they meet Client's requirements and legal obligations under any applicable laws.