STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 1

CONTRACT #: AR2437

Starting Date: 9/27/2017

Expiration Date: 9/15/2026

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and CDW Government LLC (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

Amend Attachment A to replace the prior Attachment A with the Attachment A attached to this Amendment #1.

Amend Attachment C adding the attached updated price rate list. Additionally, future catalog updates must be submitted to the Lead State of Utah for approval and will then be posted on the Contractor's landing page on the NASPO ValuePoint website here: https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/cdw-government-llc/

Parties agree all catalogs and price lists submitted by the contractor, approved by the Lead State of Utah, and posted on NASPO ValuePoint's website are incorporated by reference to this Master Agreement as Attachment C. All End User Agreements submitted by the contractor, approved by the Lead State of Utah, and posted on NASPO ValuePoint's website are incorporated by reference to this Master Agreement as Attachment E.

Effective Date of Amendment: 3/1/2024

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

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

CONTRACTOR		STATE OF UTAH	
DocuSigned by: Dario Bertocchi E290BCB577CC445...	2/29/2024	DocuSigned by: C38BE9DAC528424...	3/1/2024
Contractor's Signature	Date	Director, State of Utah Division of Purchasing	Date
Dario Bertocchi			
Contractor's Name (Print)			
VP Contracting Operations			
Title (Print)			

For Division of Purchasing Internal Use

Purchasing Agent	Phone #	E-mail Address	Contract #
Blake Theo Porter	801-957-7136	btporter@utah.gov	AR2437

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 (AR2437), 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;
(5) Appendix A to the NASPO ValuePoint Enterprise Agreement for Government Partners ("GPEA") and(6) 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.

Cloud Services means collectively and/or individually SaaS, IaaS, and/or PaaS.

Confidential Information is non-public information that is designated confidential or that a reasonable person should understand to be confidential including (1) Customer Data (2) any Purchasing Entity's records, (3) personnel records, and (4) information concerning individuals. . Confidential Information does not include information that (a) becomes publicly available without a breach of this agreement, (b) was lawfully known or received by the receiving party and specifically designated as non-confidential by the sender including all Customer Data, or (c) is a comment or suggestion one party volunteers about the other's business, products or services.

Contractor means the person or entity providing services other than Cloud Services 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.

Customer Data means all data, including all text, sound, software, or image files that are provided to by, or on behalf of, an Enrolled Affiliate through its use of the Online Services. All references to "Data" in the Master Agreement shall be deemed to mean Customer Data.

Data Breach *See defined term for Security Incident.*

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

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 by a third-party to the consumer to deploy onto the cloud infrastructure consumer created or -acquired applications created using programming languages and tools supported by a third-party 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 Cloud Services, Services, software, and any incidental tangible goods.

Protected Health Information (PHI) shall have the same meaning as the term "protected health information" in 45 CRF CFR § 160.103 of HIPAA.

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 other than Cloud Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means any unlawful access, use, theft or destruction to any Customer Data stored on third-party provider's equipment or in third-party provider's facilities, or unauthorized access to such equipment or facilities resulting in use, theft, loss, disclosure, alteration or destruction of Customer Data. All references to "Data Breach" in the Master Agreement shall be deemed to mean Security Incident.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the provider of Services 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 provider of Services. 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 by a third-party to the consumer to use applications running on a third-party'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: The initial term of this Master Agreement is for ten (10) years with no renewal options.

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 sixty (60) days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon thirty (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 if default cannot be reasonably cured as allowed per Defaults and Remedies (section 10).

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 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 of Contractor's Employees 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.

e. Notwithstanding the foregoing, damages attributable to Security Incidents shall be subject to the Section of the Master Agreement titled "Limitation of Liability."

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or 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 either party to this Master Agreement or to a Participating State or Purchasing Entity, or the appointment of a receiver or similar officer for any such party or any of such party's 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, the party claiming default shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which the defaulting party shall have an opportunity to cure the default. The 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 a defaulting party is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, the defaulting party shall be in breach of its obligations under this Master Agreement and non-defaulting party 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) In the event of default by the Contractor, and to the extent permitted by the law of the Participating State or Purchasing Entity, the Lead State shall have the right to 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. Subject to the exceptions below and the NASPO ValuePoint Participants' (as defined below) compliance with the notice and defense provisions below, in the event of any defect or deficiency in any Contractor Products or Services purchased by a Participating Entity or Purchasing Entity, Contractor agrees to defend, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees (collectively, the "NASPO Value Point Participants") against third party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property suffered by such third party and caused by the negligence, or willful misconduct of Contractor, its employees or subcontractors or volunteers, at any tier, during the performance of this Master Agreement (a "PI Claim"). This clause shall not be construed to bar any legal remedies Contractor may have with respect to the NASPO Participants' failure to fulfill their obligations pursuant to the Master Agreement or any Participating Addendum. To qualify for such defense, the Participating Entities/Purchasing Entities shall promptly notify Contractor of any PI Claim of which the Participating Entities/Purchasing Entities become aware which may give rise to a right of defense pursuant to this Section. Notice of any PI Claim that is a legal proceeding, by suit or otherwise, must be provided to Contractor within sixty (60) days of the Participating Entities'/Purchasing Entities' first learning of such proceeding. If the Participating Entity's/Purchasing Entity's laws require approval of a third party to defend Participating Entity/Purchasing Entity, Participating Entity/Purchasing Entity will seek such approval and if approval is not received, Contractor is not required to defend that Participating Entity/Purchasing Entity. If a PI Claim is settled, to the extent permitted by law, the Participating Entities/Purchasing Entities shall not publicize the settlement and will cooperate with Contractor so that Contractor can make every effort to ensure the settlement agreement contains a nondisclosure provision. Notwithstanding anything to the contrary contained herein, Participating Entities/Purchasing Entities agree that Contractor has no obligation for any PI Claim covered by this Section arising out of or resulting from the Participating Entities'/Purchasing Entities' or any of their respective employees', contractors' or agents' acts of negligence, gross negligence or misconduct. THE FOREGOING SHALL CONSTITUTE EACH AND EVERY PARTICIPATING ENTITY'S/PURCHASING ENTITY'S SOLE REMEDY AND CONTRACTOR'S SOLE AND EXCLUSIVE LIABILITY FOR ALL PI CLAIMS.

b. Indemnification – Intellectual Property. Subject to the NASPO Participant's compliance with the notice and defense requirements and exceptions set forth below, Contractor agrees to defend the NASPO Participants against any claims made by an unaffiliated third party that any Product or Service or its proper or reasonably expected or acceptable use infringes that third party's patent, copyright, or trademark or makes unlawful use of its trade secret (an "Intellectual Property Claim").

(1) The Contractor's obligations under this section shall not extend to any claims based on:

(a) Contractor's compliance with a Participating Entity's/Purchasing Entity's designs, specifications or instructions; or

(b) Contractor's use of technical information or technology provided by the Participating Entity/Purchasing Entity; or

(c) Non-Contractor software, modifications a Participating Entity/Purchasing Entity makes to, or any specifications or materials a Participating Entity/Purchasing Entity provides or makes available for, a Product; or

(d) Participating Entity's/Purchasing Entity's combination of the Product or Service with a Non-Contractor product, data or business process; or damages based on the use of a Non-Contractor product, data or business process; or

(e) Participating Entity's/Purchasing Entity's use of either Contractor's trademarks or the use or redistribution of a Product or Service in violation of this Master Agreement, Participating Addendum, or any other agreement incorporating its terms; or

(f) Participating Entity's/Purchasing Entity's use of a Product or Service after Contractor notifies Participating Entity/Purchasing Entity to discontinue that use due to a third party claim.

(2) To qualify for such defense, the involved NASPO Participants (the "Indemnified Party") shall promptly notify the Contractor of any Intellectual Property Claim of which the Indemnified Party become aware which may give rise to right of defense pursuant to this Section. Notice of any Intellectual Property Claim that is a legal proceeding, by suit or otherwise, must be provided to Contractor within sixty (60) days of the Indemnified Party's learning of such proceeding. If the Indemnified Party's laws require approval of a third party to defend the Indemnified Party, the Indemnified Party will seek such approval and if approval is not received, Contractor is not required to defend that Indemnified Party. In the event the Indemnified Party does not authorize sole control to Contractor over any claims that may arise under this subsection, then the parties agree that Contractor will be granted authorization to equally participate in any proceeding subject to this subsection. 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.

If Contractor reasonably believes that a Product or Service may infringe or misappropriate a third-party's intellectual property rights, Contractor will seek to:

i. procure for Participating Entities/Purchasing Entities the right to continue to use the Product or Service; or

ii. modify or replace it with a functional equivalent to make it non-infringing and notify Participating Entities/Purchasing Entities to discontinue use of the prior version, which Participating Entities/Purchasing Entities must do immediately.

If the foregoing options are not commercially reasonable for Contractor, or if required by a valid judicial or government order, Contractor may terminate Participating Entities'/Purchasing Entities' license or access rights in the Product or Service. In such a case, Contractor will provide Participating Entities/Purchasing Entities with notice and refund any amounts Participating Entities/Purchasing Entities have paid for those rights to the Product or Service.

THE FOREGOING SHALL CONSTITUTE THE LEAD STATE'S AND EACH AND EVERY PARTICIPATING AND/OR PURCHASING ENTITYS' SOLE REMEDY AND CONTRACTOR'S SOLE AND EXCLUSIVE LIABILITY FOR ALL INTELLECTUAL PROPERTY CLAIMS.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees

not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

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

16. Insurance

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

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no 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, limits may be met in conjunction with primary and excess/umbrella insurance coverage;

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

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

(4)

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

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

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

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

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

17. Laws and Regulations: Contractor will agree to comply with all Federal and State laws applicable to it as a corporation and as an IT Service Provider.

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

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

19. Ordering

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.

20. 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 Office3.

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

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

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

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

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell 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.

21. Payment: 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.

22. 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 where applicable to Services, 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.

23. [Intentionally deleted.]

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

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it. 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, Customer Data, or meta data 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.

26. 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.

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

28. 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.

29. Title to Product: Reserved.

30. Data Privacy: Contractor must comply with all applicable laws related to data privacy and security. Refer to Attachment E, Appendix A to the NASPO VAluePoint Enterprise Agreement for Government Partners ("GPEA"), governing data privacy as applicable to Exhibit 1 to Attachment A Software as a Service, Exhibit 2 to Attachment A Platform as A service, and Exhibit 3 to Attachment A Infrastructure as a Service. The Contractor must comply with all applicable laws.

31. 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.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. 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.

33. Waiver of Breach: Failure of a party 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 a party must be in writing. Waiver by a party 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.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any 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.

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

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for 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."

37. Governing Law and Venue

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

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the 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.

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

40. 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.

41. 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.

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

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

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

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

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

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

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

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

a. 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.

b. 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.

c. 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.

d. The Limitation of liability in section 43 will not apply to claims for liability for damages caused by a party's (i) reckless misconduct, gross negligence, willful misconduct and/or fraud (provided that, in jurisdictions that do not recognize a legal distinction between "gross negligence" and "negligence," "gross negligence" as used in this subsection shall mean "recklessness"); (ii) liability for violation of its confidentiality obligations (except obligations related to Customer Data) or the other party's intellectual property rights; or (iii) bodily injury or death.

44. 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 Attachment A of AR2473 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. Refer to Attachment E GPEA, which governs data encryption.

d. Reserved.

e. The parties agree that: (1) metadata is owned and retained by Contractor; (2) no form of Customer Data or metadata is used for any purpose other than operating and supporting the Online Services; and (3) disclosure of Customer Data to law enforcement is subject to law, but is protected by Contractor according to the terms and conditions cited in both Appendix A and Appendix C to the GPEA and in the Microsoft Online Services Terms .

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: Certain In-Scope Services include both "Enterprise Plans" and "Government Plans." Such Government Plans may also be referred to as the "Government Community Cloud Services" offerings. As of the Effective Dates, Government Community Cloud Services Offerings, as identified in

the Product Terms and OST, include a subset of Office 365 Services, Azure Core Platform Services, and Dynamics CRM Online Services (each, as defined in the DPT).

A Purchasing Entity may be provisioned for either Enterprise Plans or Government Plans, but not as a mixture of both. Once a Purchasing Entity's tenant is provisioned either for Enterprise Plan(s) or Government Plans, it will remain so for the duration of the subscription term, including renewal terms. Purchasing Entity cannot migrate between these Plans.

As exceptions to the Foregoing

(a) Customer Data will not be migrated between tenants by Microsoft pursuant to this Agreement (although in some cases Customer Data may be migrated pursuant to a separate, paid professional services agreement with Microsoft or another qualified company);

(b) Each individual tenant may be provisioned either for Enterprise Plans or Government Plans, but not both; and

(c) Purchasing Entity may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain.

All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights and this Amendment. Additionally:

(i) Government Community Cloud Services will be offered only within the United States.

(ii) Additional European Terms and the Standard Contractual Clauses, as set forth in the Use Rights, will not apply to Government Community Cloud Services.

(iii) References to geographic areas in the DPT with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.

(iv) Notwithstanding the DPT section of the OST, Azure Government Services are not subject to the same control standards and frameworks as the Microsoft Azure Core Services. The Microsoft Azure Trust Center describes the control standards and frameworks with which Azure Government Services comply.

Specifically for the Government Community Cloud Services versions of the DPT Services Office 365 Services (Exchange Online, SharePoint Online, and Skype For Business Online, when sold as part of Office 365 for Government) and Dynamics CRM Online Services (Dynamics CRM Online Services for Government), the following shall apply:

(i) Purchasing Entity Content is stored at rest in an encrypted form only within the United States.

(ii) Access to Purchasing Entity Content by Microsoft Personnel who reside outside the United States, including access to Purchasing Entity Content by authorized support staff in identified support

centers, is prohibited except in very limited circumstances permitted by written Microsoft asset handling and access standards. Any such access permitted under the foregoing Microsoft standards shall occur only after commercially reasonable efforts have been made by Microsoft to perform the function necessitating Purchasing Entity Content access with employees who reside within the United States. (e.g. vacation or other specialist staff absence coverage). In cases when it occurs, all Purchasing Entity Content access granted shall provide the minimum access necessary, for the minimum time necessary, to Microsoft personnel who reside outside the United States. Further, Purchasing Entity shall be notified of each instance of this necessitated access by Microsoft Personnel who reside outside the Untied States.

(iii) Other than as permitted in subsection (ii), above, 24x7 support staff for Government Community Cloud Services outside the United States may access Customer Data, limited solely to the following: (1) names, email addresses and other contact information for Purchasing Entity's Tenant Administrators, and Purchasing Entity's domain names, will be made available to support staff; and (2) in some cases, Purchasing Entity personnel who contact such support staff may remotely display their screens to the support staff. All other types of Customer Data will only be accessed solely by US Persons. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

4. Security Incident or Data Breach Notification:

Contractor will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Contractor is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Contractor does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Security Incident Notification

If Contractor becomes aware of any unlawful access to any Customer Data stored on Contractor's equipment or in Contractor's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Contractor will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Contractor selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Contractor's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Contractor of any fault or liability with respect to the Security Incident.

Customer must notify Contractor promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

As an exception to the foregoing, notification of Security Incident will be delivered within 5 days after Contractor determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, the State must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);

2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:

a. Name;

b. Title;

c. Email address registered as an administrator on the Online Services;

d. Email address not registered as a user on the Online Services;

3) Name of Purchasing Entity;

4) Enrollment number assigned by Contractor to represent Purchasing Entity's Tenant or Azure Subscription, on Offeror's subcontract with Contractor.

Contractor expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Contractor, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Additional language pertaining to reimbursements of costs:

To the extent that a Security Incident results from Contractor's failure to comply with its obligations under this Master Agreement (and, where applicable, Participating Addenda), and subject to the limitations of liability set forth in Attachment A, Section 43 (Limitation of Liability), Contractor will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's

obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Contractor's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Contractor under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in Attachment A, Section 43 (Limitation of Liability).

5. Personal Data Breach Responsibilities: Refer to Section 4 Security Incident or Data Breach Notification

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: Background checks will be governed by Section 8 of Attachment E to the GPEA.

9. Access to Security Logs and Reports: For the Online Services included in the Data Processing Terms section of the Microsoft Online Services Terms, Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Contractor shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

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:

Contractor Audits of Online Services

For each Online Service, Contractor will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.

- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

- Each audit will be performed by qualified, independent, third party security auditors at Contractor's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Contractor's Confidential Information. The Microsoft Audit Report will clearly disclose any material

findings by the auditor. Contractor will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If a Purchasing Entity requests, Contractor will provide the Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Contractor's compliance with the security obligations under the Data Processing Terms (DPT) section of the Microsoft Online Services Terms. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Contractor and the auditor.

12. Change Control and Advance Notice: Contractor does not charge extra for new and updated features added to any given subscription-licensed "plan" for its Online Service. However, Microsoft may reasonably choose to create new license plans in order to monetize new features and functionality.

13. Security: Security requirements are governed by Section 8.B of Appendix A to the GPEA (Attachment E).

14. Non-disclosure and Separation of Duties: Non-disclosure and Separation of duties are governed by the Online Services Terms ("OST") included in the GPEA.

15. Import and Export of Data: Section 3 of Attachment E to the GPEA (Customer Data), shall govern the import and export of Data.

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 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:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in

applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Contractor maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Contractor stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

- Contractor has specific procedures in place governing access to copies of Customer Data.

- Contractor reviews data recovery procedures at least every six months.

- Contractor logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Contractor will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Contractor shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Contractor customers and their data, or would compromise the security of the Office 365 Services, will be withheld. For clarity, “data restoration efforts” does not include automated Customer Data recovery processes such as when one of Contractor’s datacenters is activated upon failure of another.

20. Compliance with Accessibility Standards: Compliance and Accessibility Standards shall be governed by section 8.A of Attachment E to the GPEA.

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: To whatever extent a form or use of encryption is required of Contractor pursuant to any of the industry and Federal government standards committed by Contractor in this Master Agreement and the Microsoft Online Services Terms, Contractor will comply with such requirements.

23. Subscription Terms: Subscription Terms shall be governed Section 8.G of Attachment E to the GPEA.

Exhibit 2 to Attachment A of AR2473 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. Refer to Attachment E GPEA, which governs data encryption.

d. Reserved.

e. The parties agree that: (1) metadata is owned and retained by Contractor; (2) no form of Customer Data or metadata is used for any purpose other than operating and supporting the Online Services; and (3) disclosure of Customer Data to law enforcement is subject to law, but is protected by Contractor according to the terms and conditions cited in both Appendix A and Appendix C to the GPEA and in the Microsoft Online Services Terms .

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: Certain In-Scope Services include both "Enterprise Plans" and "Government Plans." Such Government Plans may also be referred to as the "Government Community Cloud Services" offerings. As of the Effective Dates, Government Community Cloud Services Offerings, as identified in

the Product Terms and OST, include a subset of Office 365 Services, Azure Core Platform Services, and Dynamics CRM Online Services (each, as defined in the DPT).

A Purchasing Entity may be provisioned for either Enterprise Plans or Government Plans, but not as a mixture of both. Once a Purchasing Entity's tenant is provisioned either for Enterprise Plan(s) or Government Plans, it will remain so for the duration of the subscription term, including renewal terms. Purchasing Entity cannot migrate between these Plans.

As exceptions to the Foregoing

(a) Customer Data will not be migrated between tenants by Microsoft pursuant to this Agreement (although in some cases Customer Data may be migrated pursuant to a separate, paid professional services agreement with Microsoft or another qualified company);

(b) Each individual tenant may be provisioned either for Enterprise Plans or Government Plans, but not both; and

(c) Purchasing Entity may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain.

All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights and this Amendment. Additionally:

(i) Government Community Cloud Services will be offered only within the United States.

(ii) Additional European Terms and the Standard Contractual Clauses, as set forth in the Use Rights, will not apply to Government Community Cloud Services.

(iii) References to geographic areas in the DPT with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.

(iv) Notwithstanding the DPT section of the OST, Azure Government Services are not subject to the same control standards and frameworks as the Microsoft Azure Core Services. The Microsoft Azure Trust Center describes the control standards and frameworks with which Azure Government Services comply.

Specifically for the Government Community Cloud Services versions of the DPT Services Office 365 Services (Exchange Online, SharePoint Online, and Skype For Business Online, when sold as part of Office 365 for Government) and Dynamics CRM Online Services (Dynamics CRM Online Services for Government), the following shall apply:

(i) Purchasing Entity Content is stored at rest in an encrypted form only within the United States.

(ii) Access to Purchasing Entity Content by Microsoft Personnel who reside outside the United States, including access to Purchasing Entity Content by authorized support staff in identified support

centers, is prohibited except in very limited circumstances permitted by written Microsoft asset handling and access standards. Any such access permitted under the foregoing Microsoft standards shall occur only after commercially reasonable efforts have been made by Microsoft to perform the function necessitating Purchasing Entity Content access with employees who reside within the United States. (e.g. vacation or other specialist staff absence coverage). In cases when it occurs, all Purchasing Entity Content access granted shall provide the minimum access necessary, for the minimum time necessary, to Microsoft personnel who reside outside the United States. Further, Purchasing Entity shall be notified of each instance of this necessitated access by Microsoft Personnel who reside outside the Untied States.

(iii) Other than as permitted in subsection (ii), above, 24x7 support staff for Government Community Cloud Services outside the United States may access Customer Data, limited solely to the following: (1) names, email addresses and other contact information for Purchasing Entity's Tenant Administrators, and Purchasing Entity's domain names, will be made available to support staff; and (2) in some cases, Purchasing Entity personnel who contact such support staff may remotely display their screens to the support staff. All other types of Customer Data will only be accessed solely by US Persons. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

4. Security Incident or Data Breach Notification: Contractor will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Contractor is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Contractor does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Security Incident Notification

If Contractor becomes aware of any unlawful access to any Customer Data stored on Contractor's equipment or in Contractor's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Contractor will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Contractor selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Contractor's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Contractor of any fault or liability with respect to the Security Incident.

Customer must notify Contractor promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

As an exception to the foregoing, notification of Security Incident will be delivered within 5 days after Contractor determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, the State must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);

2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:

a. Name;

b. Title;

c. Email address registered as an administrator on the Online Services;

d. Email address not registered as a user on the Online Services;

3) Name of Purchasing Entity;

4) Enrollment number assigned by Contractor to represent Purchasing Entity's Tenant or Azure Subscription, on Offeror's subcontract with Contractor.

Contractor expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Contractor, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Additional language pertaining to reimbursements of costs:

To the extent that a Security Incident results from Contractor's failure to comply with its obligations under this Master Agreement (and, where applicable, Participating Addenda), and subject to the limitations of liability set forth in Attachment A, Section 43 (Limitation of Liability), Contractor will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's

obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Contractor's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Contractor under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in Attachment A, Section 43 (Limitation of Liability).

5. Personal Data Breach Responsibilities : Refer to Section 4 Security Incident or Data Breach Notification.

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: Background checks will be governed by Section 8 of Attachment E to the GPEA.

9. Access to Security Logs and Reports:

For the Online Services included in the Data Processing Terms section of the Microsoft Online Services Terms, Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Contractor shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

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:

Contractor Audits of Online Services

For each Online Service, Contractor will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.

- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

- Each audit will be performed by qualified, independent, third party security auditors at Contractor's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Contractor's Confidential Information. The Microsoft Audit Report will clearly disclose any material

findings by the auditor. Contractor will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If a Purchasing Entity requests, Contractor will provide the Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Contractor's compliance with the security obligations under the Data Processing Terms (DPT) section of the Microsoft Online Services Terms. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Contractor and the auditor.

12. Change Control and Advance Notice: Contractor does not charge extra for new and updated features added to any given subscription-licensed "plan" for its Online Service. However, Microsoft may reasonably choose to create new license plans in order to monetize new features and functionality.

13. Security: Security requirements are governed by Section 8.B of Appendix A to the GPEA (Attachment E).

14. Non-disclosure and Separation of Duties: Non-disclosure and Separation of duties are governed by the Online Services Terms ("OST") included in the GPEA.

15. Import and Export of Data: Section 3 of Attachment E to the GPEA (Customer Data), shall govern the import and export of Data

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, 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:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Contractor maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Contractor stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

- Contractor has specific procedures in place governing access to copies of Customer Data.

- Contractor reviews data recovery procedures at least every six months.

- Contractor logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Contractor will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Contractor shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Contractor customers and their data, or would compromise the security of the Office 365 Services, will be withheld. For clarity, "data restoration efforts" does not include automated Customer Data recovery processes such as when one of Contractor's datacenters is activated upon failure of another..

19. Compliance with Accessibility Standards: Compliance and Accessibility Standards shall be governed by section 8.A of Attachment E. to the GPEA.

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: To whatever extent a form or use of encryption is required of Contractor pursuant to any of the industry and Federal government standards committed by Contractor in this Master Agreement and the Microsoft Online Services Terms, Contractor will comply with such requirements.

22. Subscription Terms: Subscription Terms shall be governed Section 8.G of Attachment E to the GPEA.

Exhibit 3 to Attachment A of AR2473 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. Refer to Attachment E GPEA, which governs data encryption.

d. Reserved.

e. The parties agree that: (1) metadata is owned and retained by Contractor; (2) no form of Customer Data or metadata is used for any purpose other than operating and supporting the Online Services; and (3) disclosure of Customer Data to law enforcement is subject to law, but is protected by Contractor according to the terms and conditions cited in both Appendix A and Appendix C to the GPEA and in the Microsoft Online Services Terms .

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: Certain In-Scope Services include both "Enterprise Plans" and "Government Plans." Such Government Plans may also be referred to as the "Government Community Cloud Services" offerings. As of the Effective Dates, Government Community Cloud Services Offerings, as identified in

the Product Terms and OST, include a subset of Office 365 Services, Azure Core Platform Services, and Dynamics CRM Online Services (each, as defined in the DPT).

A Purchasing Entity may be provisioned for either Enterprise Plans or Government Plans, but not as a mixture of both. Once a Purchasing Entity's tenant is provisioned either for Enterprise Plan(s) or Government Plans, it will remain so for the duration of the subscription term, including renewal terms. Purchasing Entity cannot migrate between these Plans.

As exceptions to the Foregoing

(a) Customer Data will not be migrated between tenants by Microsoft pursuant to this Agreement (although in some cases Customer Data may be migrated pursuant to a separate, paid professional services agreement with Microsoft or another qualified company);

(b) Each individual tenant may be provisioned either for Enterprise Plans or Government Plans, but not both; and

(c) Purchasing Entity may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain.

All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights and this Amendment. Additionally:

(i) Government Community Cloud Services will be offered only within the United States.

(ii) Additional European Terms and the Standard Contractual Clauses, as set forth in the Use Rights, will not apply to Government Community Cloud Services.

(iii) References to geographic areas in the DPT with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.

(iv) Notwithstanding the DPT section of the OST, Azure Government Services are not subject to the same control standards and frameworks as the Microsoft Azure Core Services. The Microsoft Azure Trust Center describes the control standards and frameworks with which Azure Government Services comply.

Specifically for the Government Community Cloud Services versions of the DPT Services Office 365 Services (Exchange Online, SharePoint Online, and Skype For Business Online, when sold as part of Office 365 for Government) and Dynamics CRM Online Services (Dynamics CRM Online Services for Government), the following shall apply:

(i) Purchasing Entity Content is stored at rest in an encrypted form only within the United States.

(ii) Access to Purchasing Entity Content by Microsoft Personnel who reside outside the United States, including access to Purchasing Entity Content by authorized support staff in identified support

centers, is prohibited except in very limited circumstances permitted by written Microsoft asset handling and access standards. Any such access permitted under the foregoing Microsoft standards shall occur only after commercially reasonable efforts have been made by Microsoft to perform the function necessitating Purchasing Entity Content access with employees who reside within the United States. (e.g. vacation or other specialist staff absence coverage). In cases when it occurs, all Purchasing Entity Content access granted shall provide the minimum access necessary, for the minimum time necessary, to Microsoft personnel who reside outside the United States. Further, Purchasing Entity shall be notified of each instance of this necessitated access by Microsoft Personnel who reside outside the Untied States.

(iii) Other than as permitted in subsection (ii), above, 24x7 support staff for Government Community Cloud Services outside the United States may access Customer Data, limited solely to the following: (1) names, email addresses and other contact information for Purchasing Entity's Tenant Administrators, and Purchasing Entity's domain names, will be made available to support staff; and (2) in some cases, Purchasing Entity personnel who contact such support staff may remotely display their screens to the support staff. All other types of Customer Data will only be accessed solely by US Persons. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

4. Security Incident or Data Breach Notification: Contractor will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Contractor is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Contractor does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Security Incident Notification

If Contractor becomes aware of any unlawful access to any Customer Data stored on Contractor's equipment or in Contractor's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Contractor will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Contractor selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Contractor's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Contractor of any fault or liability with respect to the Security Incident.

Customer must notify Contractor promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

As an exception to the foregoing, notification of Security Incident will be delivered within 5 days after Contractor determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, the State must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);

2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:

a. Name;

b. Title;

c. Email address registered as an administrator on the Online Services;

d. Email address not registered as a user on the Online Services;

3) Name of Purchasing Entity;

4) Enrollment number assigned by Contractor to represent Purchasing Entity's Tenant or Azure Subscription, on Offeror's subcontract with Contractor.

Contractor expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Contractor, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Additional language pertaining to reimbursements of costs:

To the extent that a Security Incident results from Contractor's failure to comply with its obligations under this Master Agreement (and, where applicable, Participating Addenda), and subject to the limitations of liability set forth in Attachment A, Section 43 (Limitation of Liability), Contractor will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's

obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Contractor's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Contractor under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in Attachment A, Section 43 (Limitation of Liability).

5. Personal Data Breach Responsibilities: Refer to Section 4 Security Incident or Data Breach Notification.

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: Background checks will be governed by Section 8 of Attachment E to the GPEA

9. Access to Security Logs and Reports: For the Online Services included in the Data Processing Terms section of the Microsoft Online Services Terms, Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Contractor shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

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: Contractor Audits of Online Services

For each Online Service, Contractor will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Contractor's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Contractor's Confidential Information. The Microsoft Audit Report will clearly disclose any material

findings by the auditor. Contractor will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If a Purchasing Entity requests, Contractor will provide the Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Contractor's compliance with the security obligations under the Data Processing Terms (DPT) section of the Microsoft Online Services Terms. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Contractor and the auditor.

12. Change Control and Advance Notice: Contractor does not charge extra for new and updated features added to any given subscription-licensed "plan" for its Online Service. However, Microsoft may reasonably choose to create new license plans in order to monetize new features and functionality.

13. Security: Security requirements are governed by Section 8.B of Appendix A to the GPEA (Attachment E).

14. Non-disclosure and Separation of Duties: Non-disclosure and Separation of duties are governed by the Online Services Terms ("OST") included in the GPEA.

15. Import and Export of Data: Section 3 of Attachment E to the GPEA (Customer Data), shall govern the import and export of Data.

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 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:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Contractor maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Contractor stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

- Contractor has specific procedures in place governing access to copies of Customer Data.

- Contractor reviews data recovery procedures at least every six months.

- Contractor logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Contractor will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Contractor shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Contractor customers and their data, or would compromise the security of the Office 365 Services, will be withheld. For clarity, "data restoration efforts" does not include automated Customer Data recovery processes such as when one of Contractor's datacenters is activated upon failure of another.

19. **Subscription Terms:** Subscription Terms shall be governed Section 8.G of Attachment E to the GPEA.

Attachment C
CDW Government, LLC (CDW-G)
NASPO ValuePoint Cloud Solutions
Master Agreement # AR2473

Cloud Solutions By Category	
Solution	**Minimum Discount from MSRP %**
Software as a Service	1%
Infrastructure as a Service	1%
Platform as a Service	1%
Value Added Services*	1%

** These incorporate services to support the Software as a Service, Platform as a Service, and Infrastructure as a Service, offerings. This also incorporates stand alone professional services including staff aug, provided by CDW-G.*

CDW Government, LLC (CDW-G)

NASPO ValuePoint Cloud Solutions
Master Agreement # AR2473

Digital Velocity Services (DVS)		
Role	**Hourly Rate, minimum**	**Hourly Rate, maximum**
DVS F-CTO	$350.00	$386.33
DVS Digital Strategy Consultant	$305.00	$336.66
DVS Digital Product Strategist	$270.00	$298.03
DVS Principal Engineer / Tech. Lead	$350.00	$386.33
DVS Architect	$300.00	$331.14
DVS Senior Engineer	$250.00	$275.95
DVS Engineer	$225.00	$248.36
DVS Associate Engineer	$200.00	$220.76
DVS Program Manager	$245.00	$270.43
DVS Sr. Technical Project Manager	$230.00	$253.88
DVS Technical Project Manager	$210.00	$231.80
DVS Project Coordinator	$165.00	$182.13

ServiceNow Solutions Services		
Role	**Hourly Rate, minimum**	**Hourly Rate, maximum**
ServiceNow Associate Project Coordinator Manager	$165	$182
ServiceNow Associate Developer	$170	$188
ServiceNow Associate Solution Architect	$245	$270
ServiceNow Business Analyst	$200	$221
ServiceNow Business Process Consultant	$310	$342
ServiceNow Developer	$220	$243
ServiceNow Developer Automation	$220	$243
ServiceNow Developer Offshore	$120	$132
ServiceNow Engagement Manager	$275	$304
ServiceNow Innovation Consultant	$310	$342
ServiceNow Integration Expert	$290	$320
ServiceNow Master Architect	$350	$386
ServiceNow Portfolio Manager	$350	$386
ServiceNow Principal Consultant	$310	$342
ServiceNow Program Manager	$300	$331
ServiceNow Quality Assurance Expert	$225	$248
ServiceNow Scrum Master	$220	$243
ServiceNow Service Coordinator	$165	$182
ServiceNow Service Management Advisor	$310	$342
ServiceNow Solution Architect	$290	$320
ServiceNow Subcontractor – Align Financials	$297	$328
ServiceNow Supervisor	$290	$320
ServiceNow Technical Architect	$350	$386
ServiceNow Technical Consultant	$245	$270
ServiceNow Trainer	$265	$293

Staff Augmentation Services						
Role	**Standard, minimum**	**Standard, maximum**	**Mid-Level, minimum**	**Mid-Level, maximum**	**Senior, minimum**	**Senior, maximum**
Infrastructure Architects	$170.00	$187.65	$180.00	$198.69	$195.00	$215.24
Solutions Architects	$175.00	$193.17	$195.00	$215.24	$215.00	$237.32
Site Reliability Engineers	$185.00	$204.21	$195.00	$215.24	$205.00	$226.28
Network Administrators	$100.00	$110.38	$115.00	$126.94	$125.00	$137.98
Network Engineers	$135.00	$149.01	$150.00	$165.57	$165.00	$182.13
Network BAs/BSAs	$130.00	$143.50	$135.00	$149.01	$140.00	$154.53
Systems Administrators	$115.00	$126.94	$130.00	$143.50	$145.00	$160.05
Systems Engineers	$140.00	$154.53	$155.00	$171.09	$170.00	$187.65
Systems BAs/BSAs	$135.00	$149.01	$145.00	$160.05	$155.00	$171.09
Storage Engineers	$165.00	$182.13	$160.00	$176.61	$195.00	$215.24
Virtualization Engineers	$135.00	$149.01	$155.00	$171.09	$180.00	$198.69
Salesforce Administrators	$125.00	$137.98	$155.00	$171.09	$185.00	$204.21
Salesforce Engineers	$175.00	$193.17	$195.00	$215.24	$215.00	$237.32
Salesforce Developers	$165.00	$182.13	$175.00	$193.17	$185.00	$204.21
SolarWinds Engineers	$165.00	$182.13	$180.00	$198.69	$205.00	$226.28
AWS Engineers	$185.00	$204.21	$205.00	$226.28	$225.00	$248.36
AWS Developers	$170.00	$187.65	$175.00	$193.17	$180.00	$198.69
Azure Engineers	$180.00	$198.69	$195.00	$215.24	$215.00	$237.32
Azure Developers	$135.00	$149.01	$145.00	$160.05	$160.00	$176.61
GCP Engineers	$200.00	$220.76	$235.00	$259.40	$265.00	$292.51
GCP Developers	$200.00	$220.76	$235.00	$259.40	$265.00	$292.51
Front-end Developers	$165.00	$182.13	$170.00	$187.65	$175.00	$193.17
Back-end Developers	$170.00	$187.65	$180.00	$198.69	$185.00	$204.21
Scala Developers	$200.00	$220.76	$215.00	$237.32	$225.00	$248.36
Project Managers	$135.00	$149.01	$150.00	$165.57	$165.00	$182.13
Scrum Masters	$165.00	$182.13	$180.00	$198.69	$195.00	$215.24
DevOps Engineers	$165.00	$182.13	$175.00	$193.17	$190.00	$209.72
Software Development Engineer in Test	$170.00	$187.65	$180.00	$198.69	$195.00	$215.24
InfoSec Analysts	$145.00	$160.05	$160.00	$176.61	$175.00	$193.17
Quality Assurance Analysts	$140.00	$154.53	$150.00	$165.57	$160.00	$176.61
Quality Assurance Engineers	$140.00	$154.53	$150.00	$165.57	$160.00	$176.61
	ServiceNow SmartTeam Staff Augmentation					
ServiceNow SmartTeam Business Process Consultant	$182	$201	N/A	N/A	$193	$213
ServiceNow SmartTeam Solution Architect	$185	$204	N/A	N/A	$206	$227
ServiceNow SmartTeam Technical Consultant	$150	$166	N/A	N/A	$167	$184
ServiceNow SmartTeam Associate Developer	$133	$147	$148	$163	$167	$184
ServiceNow SmartTeam ServiceNow Solutions Developer Offshore	$93	$103	N/A	N/A	N/A	N/A
ServiceNow SmartTeam Business Analyst	$158	$174	N/A	N/A	$167	$184

ServiceNow SmartTeam Certified Master Architect	$300	$331	N/A	N/A	N/A	N/A

Other Professional Services		
Role	**Hourly Rate, minimum**	**Hourly Rate, maximum**
Associate Consulting Engineer	$175.00	$193.17
Consulting Engineer	$215.00	$237.32
Senior Consulting Engineer	$240.00	$264.92
Technical Lead / Principal Consulting Engineer	$265.00	$292.51
Enterprise Consulting Architect	$275.00	$303.55
Business Consulting Analyst	$260.00	$286.99
Project Administrator	$165.00	$182.13
Project Manager	$210.00	$231.80
Senior Project Manager	$220.00	$242.84
Enterprise Project Manager, PMO Lead	$230.00	$253.88
Program Manager	$235.00	$259.40
Technical Architect	$350.00	$386.33
Incident Responder/Forensic Analyst	$385.00	$424.97

Amplified Services	
Google for Education (GFE)	
Option	**Discount off MSRP**
GFE Audit - K-12	2%
GFE Audit - Higher Ed	2%
GFE KickStart Package	2%
GFE Support - Support Hours	2%
GFE Support - 20 Support Hours	2%
GFE Support - 40 Support Hours	2%
GFE Support - Adhoc Support Hours	2%
North American GFE Technical Collaborative	2%
GFE Training/Consultancy - Full Day Onsite	2%
GFE Chrome Checkup	2%
Amplified IT Training	
Option	**Discount off MSRP**
Amplified IT Admin Level 1 Certification Training - Self-Paced	2%
Amplified IT Admin Level 2 Certification Training - Self-Paced	2%
Amplified IT Admin Security Specialist Certification Training - Self-Paced	2%
Amplified IT Admin Security Bundle	2%

Professional Serv

CDW Government, LLC (CDW-G)

NASPO ValuePoint Cloud Solutions
Master Agreement # AR2473

SaaS Offerings	
OEM	**Minimum Discount from MSRP %**
Adobe	1%
AWS	1%
Canva	1%
Cisco	1%
CrowdStrike	1%
Cyber-Ark	1%
Druva	1%
Google	1%
Gopher products	2%
IBM	1%
Ivanti, Inc.	1%
Little SIS	2%
Looker Data Sciences, Inc.	1%
Mandiant	1%
Nutanix	1%
Okta, Inc.	1%
Rubrik	1%
Sailpoint	1%
Secureworks, Inc.	1%
ServiceNow	1%
Singlewire Software	1%
Splunk	1%
Tanium Inc.	1%
Tenable Public Sector, LLC	1%
Tintri	1%
Varonis	1%
Veeam Software Corp.	1%
VMware	1%
Zscaler, Inc.	1%

Cloud offerings are constantly evolving and increasingly complex, with a range of subscription and consumption-based offerings. In cases where MSRP pricing is not available and/or the offering is unique, pricing will be based on CDW•G invoiced price. This structure provides the necessary flexibility to enable customers to make purchases as cloud offerings continue to evolve over the life of our contract

CDW Government, LLC (CDW-G)

NASPO ValuePoint Cloud Solutions
Master Agreement # AR2473

IaaS Offerings	
OEM	**Minimum Discount from MSRP %**
Google	1%
AWS	1%

Cloud offerings are constantly evolving and increasingly complex, with a range of subscription and consumption-based offerings. In cases where MSRP pricing is not available and/or the offering is unique, pricing will be based on CDW•G invoiced price. This structure provides the necessary flexibility to enable customers to make purchases as cloud offerings continue to evolve over the life of our contract

CDW Government, LLC (CDW-G)

NASPO ValuePoint Cloud Solutions
Master Agreement # AR2473

PaaS Offerings	
OEM	**Minimum Discount from MSRP %**
Google	1%
AWS	1%

Cloud offerings are constantly evolving and increasingly complex, with a range of subscription and consumption-based offerings. In cases where MSRP pricing is not available and/or the offering is unique, pricing will be based on CDW•G invoiced price. This structure provides the necessary flexibility to enable customers to make purchases as cloud offerings continue to evolve over the life of our contract