Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

State of Utah Cooperative Contract

PARTICIPATING ADDENDUM
CLOUD AND SOFTWARE SOLUTIONS

State of Utah Contract #: AR5004

Master Agreement: LS5004

Contractor: Istonish

Participating Entity: STATE OF UTAH

Participating Entity Contract: AR5004

The following products or services are included in this contract portfolio:

- All products and services listed on the Contractor page on the NASPO ValuePoint website.

Participating Addendum Terms and Conditions:

1. Scope: This addendum covers Cloud Solutions and Software Solutions led by NASPO ValuePoint for use by state agencies and other entities located in the State of Utah authorized by that State's statutes to utilize State contracts with the prior approval of the State's Chief Procurement Official. An amendment to this PA is not required when offerings are adjusted in the Master Agreement, so long as all additions remain within the master agreement's original scope.

2. Pricing: The pricing and rates from the Master Agreement shall flow down to this PA. An amendment to this PA is not required when pricing in the Master Agreement is adjusted / updated.

3. Administrative Fee: One (1) percent (1%) and will apply per Section 35 of Attachment A.

4. Contract Effective Dates: This PA is effective upon final signature of both parties and expires upon the expiration or termination of the NASPO ValuePoint. A contract amendment is not necessary in the event of the renewal or extension of the Master Agreement, so long as such renewal/extension was originally provided within the solicitation supporting the master agreement.

5. Order of Precedence:
   The order of precedence as provided in the NASPO ValuePoint Master Agreement LS5004 applies to this PA.

6. Participation: This NASPO Value Point Master Agreement may be used by all state agencies, institutions of higher institution, political subdivisions and other entities authorized to use statewide contracts in the State of Utah. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

7. Subcontractors: All contactors, dealers, and resellers authorized in the State of Utah, as shown on the dedicated Contractor (cooperative contract) website, are approved to provide sales and service support to participants in the NASPO ValuePoint Master Agreement. The Contractor's dealer participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement.
8. Orders: Any order placed by an Eligible User for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.

9. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

State of Utah Cooperative Contract

PARTICIPATING ADDENDUM
CLOUD AND SOFTWARE SOLUTIONS

State of Utah Contract #: AR5004

Contractor

Name:	Clinton Marsh
Address:	5500 Greenwood Plaza Blvd., Suite 130, Greenwood Village, CO 80111
Telephone:	303-498-0245
Email:	cmarsh@istonish.com
Vendor Number:	VC228030
Commodity Codes:	92005

State of Utah Division of Purchasing

Name:	State of Utah, Division of Purchasing, Keli Lessing
Address:	4315 South 2700 West Fl 3, Taylorsville, UT 84129-2128
Telephone:	801-957-7167
Email:	klessing@utah.gov

10. Additional Terms and Conditions:
The following terms and conditions will apply to this participating addendum.

ATTACHMENT A: STATE OF UTAH COOPERATIVE STANDARD INFORMATION TECHNOLOGY TERMS AND CONDITIONS

This is a State Cooperative Contract for information technology products and services. DTS policies referenced by number in this Attachment are only applicable to the Executive Branch and are available at https://dts.utah.gov/policies. All other policies and codes of conduct are available upon request.

1. DEFINITIONS:

a) "**Access to Secure State Facilities, Data, or Technology**" means Contractor will (a) enter upon secure premises controlled, held, leased, or occupied by State of Utah or Eligible User; (b) maintain, develop, or have access to any deployed hardware, software, firmware, or any other technology, that is in use by State of Utah or Eligible User; or (c) have access to or receive any State Data or Confidential Information.

b) "**Authorized Persons**" means the Contractor's employees, officers, partners, Subcontractors, or agents of Contractor who need Access to Secure State Facilities, Data, or Technology to enable the Contractor to perform its responsibilities under this Contract.

c) "**Background IP**" means intellectual property (IP) owned or controlled prior to the effective date of this Contract or that IP developed or acquired from activities independent of the services performed under this Contract, including but not limited to (a) methodologies, processes, technologies, algorithms, software, or development tools used in performing the Services, and (b) processes and reusable reports, designs, charts, plans, specifications, documentation, forms, templates, or output which are supplied or otherwise used by or on behalf of Contractor in the course of performing the Services or creating the Custom Deliverables, other than portions that specifically incorporate proprietary or Confidential Information or Custom Deliverables of Eligible User.

d) "**Contract**" means the Contract Signature Page(s), including all referenced attachments and documents incorporated by reference.

e) "**Contract Period**" means the term of this Contract, as set forth in the Contract Signature Page(s).

f) "**Contract Signature Page(s)**" means the cover page that the Division and Contractor sign.

g) "**Contractor**" means the individual or entity identified on the Contract Signature Page(s). "Contractor" includes Contractor's agents, officers, employees, partners, contractors, and Subcontractors at any level.

h) "**Custom Deliverables**" means the product that Contractor is required to design, develop, or customize and deliver to the Eligible User as specifically described under this Contract or an associated statement of work for which all interest and title shall be transferred to and owned by the Eligible User. This includes every invention, design, development, customization, improvement, process, software program, work of authorship,

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

documentation, formula, datum, technique, know how, or intellectual property right whatsoever or any interest therein (whether patentable or not patentable or registrable under copyright or similar statutes or subject to analogous protection) that is specifically made, conceived, discovered, or reduced to practice by Contractor pursuant to this Contract.

i) "**Data Breach**" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of State Data that compromises the security, confidentiality, or integrity of State Data.

j) "**Division**" means the State of Utah Division of Purchasing.

k) "**DTS**" means the Utah Department of Government Operations Division of Technology Services.

l) "**Eligible User(s)**" means the State of Utah's government departments, institutions, agencies, political subdivisions (i.e., colleges, school districts, counties, cities, etc.), and, as applicable, nonprofit organizations, agencies of the federal government, or any other entity authorized by the laws of the State of Utah to participate in State Cooperative Contracts.

m) "**Federal Criminal Background Check**" means a fingerprint-based, nationwide background check conducted and processed by the FBI.

n) "**Federal Data**" means all information that originated with a federal entity, including tax information.

o) "**Good**" means any deliverable not classified as a Custom Deliverable or Service.

p) "**Intellectual Property Rights**" means all rights to patents, utility models, mask works, copyrights, trademarks, trade secrets, and other protection afforded by law to inventions, models, designs, technical information, and applications.

q) **"NASPO MA"** means the underlying master agreement executed by and between the Contractor and the Division, acting as the Lead State, in cooperation with NASPO ValuePoint.

r) "**Non-Public Data**" means records or data that are not subject to distribution to the public. Access is restricted because it includes information that is protected by state or federal law. Non-Public Data includes, but is not limited to, a person's name; government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information; or Protected Health Information.

s) **"Personal Data"** means information, whether by itself or combined with other data elements, that can identify an individual with reasonable specificity or that is linked or can be reasonably linked to an identified individual.

t) "**Procurement Item**" means a Good, a supply, Services, Custom Deliverable, construction, or technology that Contractor is required to deliver to the State of Utah under this Contract, including software and Software as a Service.

u) "**Protected Health Information**" (PHI) is as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and its implementing regulations.

v) "**Response**" means the Contractor's bid, proposals, quote, or any other document used by the Contractor to respond to the State Entity's Solicitation.

w) "**Security Incident**" means the attempted unauthorized access to State Data or Personal Data that may result in the use, disclosure, or theft of State Data or Personal Data. Consistent with the GDPA at Subsection 63A-19-405(1)(b), a governmental entity must report "the unauthorized access, acquisition, disclosure, loss of access, or destruction of data that compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the governmental entity". An incident does not include unsuccessful pings and port scans.

x) "**Services**" means the furnishing of labor, time, or effort by Contractor, and may include installation, configuration, implementation, technical support, warranty maintenance, and other support services.

y) "**Solicitation**" means an invitation for bids, request for proposals, notice of sole source procurement, request for statement of qualifications, request for information, or any document used to obtain bids, proposals, pricing, qualifications, or information for the purpose of entering into this Contract.

z) "**Single Sign On**" means the authentication and authorization system operated by the State of Utah for accessing resources operated either by the State or a third party on behalf of the State.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

aa) "**X [Software, Platform, Infrastructure, Network, etc.] as a Service** " means an application running on a Contractor's or State's cloud infrastructure which is accessible from various client devices through a thin client interface (e.g. a such as a Web browser, (e.g. Web-based email), or a program interface) For clarity, the State 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.

bb) "**State Data**" means all Confidential Information, Non-Public Data, and Personal Data that is created, controlled, maintained, owned, or in any way originating from or on behalf of the State of Utah, and all State-controlled data that is the output of computer processing or other electronic manipulation of any data the State created, controlled, maintained, or in any way originated from the State of Utah, regardless of where such data or output is stored or maintained.

cc) "**State of Utah" or "State Entity" or "State"** means the State of Utah, in its entirety, including its institutions, agencies, departments, divisions, authorities and instrumentalities, boards, commissions, elected or appointed officers, employees, agents, authorized volunteers, and where applicable, Eligible Users.

dd) **"StateRAMP dba GovRAMP"** means a Risk and Authorization Management Program, which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by state and local governments, public education institutions, and special districts enabling these organizations to validate the security of their third-party IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and/or SaaS (Software as a Service) solutions which process, transmit, store the organization's data or which could impact data security GovRAMP's security verification model is based on NIST 800-53 Rev. 5 published by the National Institute of Standards and Technology (NIST). Moving forward GovRAMP will be the name used.

ee) **"GovRAMP Verified Status"** means a status indicating that a service provider has met all GovRAMP security requirements related to that status and has been provided with an authorization established by the GovRAMP governing boards including but not limited to Ready, Core, Authorized or Provisionally Authorized.

ff) **"GovRAMP Progressing Snapshot"** means a program within the GovRAMP framework that utilizes a predetermined set of NIST 800-53 controls for quarterly evaluations and monthly advisory calls. This program aims to identify and address deficiencies in the security of cloud products, ensuring continuous improvement and compliance with GovRAMP standards.

gg) "**Subcontractors**" includes contractors, manufacturers, distributors, suppliers, or consultants, at any tier, that are under the direct or indirect control or responsibility of Contractor, including a person or entity that is, or will be, providing goods or performing services pursuant to this Contract.

2. ESSENTIAL PROVISIONS:

a. **CONTRACT JURISDICTION, CHOICE OF LAW, AND VENUE:** This Contract shall be governed solely by the laws of the State of Utah. Any action or proceeding arising from this Contract shall be brought in a court of competent jurisdiction in the State of Utah. Exclusive venue shall be in Salt Lake City, in the Third Judicial District Court for Salt Lake County. (UCA § 63G-6a-1203(4)(f)(ii))

b. **LAWS:** Contractor and all Goods and Services delivered under this Contract will comply with all applicable federal and state of Utah laws, including applicable licensure and certification requirements.

c. **SOVEREIGN IMMUNITY:** The Division and the State of Utah do not waive any protection, right, defense or immunity under the Governmental Immunity Act of Utah, Utah Code §§ 63G-7-101 to 904, as amended, the Eleventh Amendment to the Constitution of the United States, or otherwise, from any claim or from the jurisdiction of any court. If a claim must be brought in a federal forum, then the party bringing the claim shall file it and seek to adjudicate it exclusively within the United States District Court for the District of Utah. This paragraph applies only to a claim brought against DTS or the State of Utah to the extent Congress has abrogated the State of Utah's sovereign immunity. Furthermore, this paragraph is not consent by DTS or the State of Utah to be sued in federal court.

d. **PUBLIC INFORMATION:** This Contract and any purchase orders, invoices, pricing lists, and the Response are public records available for disclosure in accordance with the State of Utah's Government Records Access and Management Act (GRAMA, Utah Code 63G-2-101 et seq.), except to the extent classified as protected in

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

accordance with UCA § 63G-2-309. GRAMA takes precedence over any statements of confidentiality or similar notations. Neither the Division, the Eligible User nor the State of Utah will inform Contractor of any request for a copy of this Contract, including any purchase orders, invoices, pricing lists, or the Response.

e. **CREDITING THE DIVISION IN PUBLICITY:** Any publicity given to this Contract shall identify the Division as the managing agency and shall not be released without prior written approval from the Division.

f. **SALES TAX EXEMPTION:** Goods, Custom Deliverables, and Services purchased by some Eligible Users are being paid from that Eligible User's funds and used in the exercise of that Eligible User's essential functions as a State of Utah governmental entity. Any such Eligible Users will provide Contractor with a copy of its sales tax exemption number upon request.

g. **SEVERABILITY:** A declaration or order by any court that any provision of this Contract is illegal and void shall not affect the legality and enforceability of any other provision of this Contract, unless the provisions are mutually dependent.

h. **AMENDMENTS:** This Contract may only be amended by the mutual written agreement of the parties, provided that the amendment is within the Scope of Work of this Contract, is within the scope/purpose of the Solicitation, and is attached and made part of this Contract. Automatic renewals are prohibited and are deemed void even if listed elsewhere in this Contract. (UCA § 63G-6a-1203(4)(h))

i. **DEBARMENT:** Defer to NASPO MA Terms and Conditions but for the following: If the Contractor cannot certify the statement contained in the NASPO MA Terms and Conditions, attach a written explanation for review by the Lead State.

j. **NONAPPROPRIATION OF FUNDS, REDUCTION OF FUNDS, OR CHANGES IN LAW:** This Contract may be terminated in whole or in part at the sole discretion of the Division or Eligible User upon thirty days written notice, if the Division or Eligible User determines that (a) a change in Federal or State legislation or applicable laws materially affects the ability of either party to perform under the terms of this Contract; or (b) that a change in available funds affects the Division or Eligible User's ability to pay under this Contract. A change of available funds includes, but is not limited to, a change in Federal or State funding, whether as a result of a legislative act or an order of the President, the Governor, or Executive Director.

k. The Division or Eligible User, as applicable, will reimburse Contractor for the Goods or Services properly ordered and delivered until the effective date of said notice. The Division and Eligible User are not liable for any performance, commitments, penalties, or liquidated damages that accrue after the effective date of the notice.

l. **ENTIRE AGREEMENT:** This Contract is the entire agreement between the parties, and supersedes any prior and contemporaneous agreements and understandings between the parties, whether oral or written.

m. **WAIVER:** Defer to NASPO MA Terms and Conditions.

n. **CHANGES IN SCOPE:** Any changes in the scope of work to be performed under this Contract shall be in the form of a written amendment to this Contract, mutually agreed to and signed by both parties, specifying any such changes, fee adjustments, any adjustment in time of performance, or any other significant factors arising from the changes in the scope of work.

o. **TRAVEL COSTS:** Unless otherwise agreed to in the contract, all travel costs associated with the delivery of Services will be paid in accordance with the Utah Administrative Code R25-7. Invoices containing travel costs outside of these rates will be returned to the Contractor for correction.

3. **RECORDS ADMINISTRATION:** Contractor shall maintain or supervise the maintenance of all records necessary to properly account for Contractor's performance and the payments made by an Eligible User to Contractor. These records shall be retained by Contractor for at least six (6) years after final payment (per Utah Administrative Code R33-12-605 and UCA § 78B-2-309), or until all audits initiated within the six (6) years have been completed, whichever is later. Contractor shall allow, at no additional cost, State of Utah auditors, federal auditors, Eligible Users or any firm identified by the Division, access to all such records. Contractor must refund to the Division any overcharges brought to Contractor's attention by the Division or the Division's auditor and Contractor is not permitted to offset identified overcharges by alleged undercharges to Eligible Users.

4. **CERTIFY REGISTRATION AND USE OF EMPLOYMENT "STATUS VERIFICATION SYSTEM":** This Status Verification System, also referred to as "E-verify", requirement only applies to contracts issued through a request for proposal process and to sole sources that are included within a request for proposal.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

1) Contractor certifies as to its own entity, under penalty of perjury, that Contractor has registered and is participating in the Status Verification System to verify the work eligibility status of Contractor's new employees that are employed in the State of Utah in accordance with applicable immigration laws including UCA § 63G-12-302, Utah Code, as amended.

2) Contractor shall require that the following provision be placed in each subcontract at every tier: "The subcontractor shall certify to the main (prime or general) Contractor by affidavit that the subcontractor has verified through the Status Verification System the employment status of each new employee of the respective subcontractor, all in accordance with applicable immigration laws including UCA § 63G-12-302, Utah Code, as amended, and to comply with all applicable employee status verification laws. Such affidavit must be provided prior to the notice to proceed for the subcontractor to perform the work."

3) Contractor's failure to comply with this section will be considered a material breach of this Contract.

4) Contractor shall protect, indemnify, and hold harmless the Division, the Eligible Users, and the State of Utah, and anyone that the State of Utah may be liable for, against any claim, damages, or liability arising out of or resulting from violations of the above Status Verification System Section whether violated by employees, agents, or contractors of the following: (a) Contractor; (b) Subcontractor at any tier; and/or (c) any entity or person for whom the Contractor or Subcontractor may be liable.

5. **CONFLICT OF INTEREST:** Contractor represents that none of its officers or employees are officers or employees of the State of Utah, unless written disclosure has been made to the Division.

6. **INDEPENDENT CONTRACTOR:** Defer to NASPO MA Terms and Conditions.

7. **CRIMINAL BACKGROUND SCREENING:** Depending on the Eligible User's policy, each employee of Contractor and Subcontractor may be required to successfully complete a Federal Criminal Background Check, prior to being granted Access to Secure State Facilities, State Data, or Technology. Contractor or the applicable employee shall provide Eligible Users with sufficient personal information (at Contractor's expense) so that a Federal Criminal Background Check may be completed by the Eligible User, at Eligible User's expense. The Eligible User will provide Contractor with forms which must be filled out by Contractor and returned to the Eligible User. Each employee of Contractor or a Subcontractor who will have Access to Secure State Facilities, State Data, or Technology must be fingerprinted by the Eligible User or local law enforcement a minimum of one week prior to needing access. At the time of fingerprinting, said employee shall disclose all felony or misdemeanor convictions. Eligible Users may conduct a Federal Criminal Background Check based upon the fingerprints and personal information provided and use this same information to complete a Name Check in the Utah Criminal Justice Information System (UCJIS) at least every two years. Eligible Users may revoke Access to Secure State Facilities, Data, and Technology granted in the event of any negative results. Contractor and the employee or subcontractor shall immediately notify Eligible Users if an arrest or conviction for a felony or misdemeanor of any person that has Access to Secure State Facilities, State Data or Technology occurs during the Contract Period. Eligible Users will determine in its discretion if such person's Access to Secure State Facilities, State Data, or Technology shall remain in effect. Felony and misdemeanor are defined by the laws of the State of Utah, regardless of where the conviction occurred. (DTS Policy 2000-0014 Background Investigations). Additionally, each employee, consultant of Contractor, and Subcontractor who will be granted unescorted access to Secure State Facilities, State Data, or Technology must successfully complete a 10-panel drug test at Contractor's expense with the pass/fail results of the drug test provided to the State of Utah's hiring manager prior to such access being granted. DTS may revoke Access to Secure State Facilities, Data, and Technology in the event the results of a drug test are positive. DTS will determine in its discretion if such person's Access to Secure State Facilities, State Data, or Technology shall remain in effect. Contractor's employees and any Subcontractors who have unescorted Access to Secure State Facilities or to State or Federal Data or any Access to Technology will complete at no additional cost any required security training as requested by the State. Felony and misdemeanor are defined by the laws of the State of Utah, regardless of where the conviction occurred.

8. **DRUG-FREE WORKPLACE:** Contractor shall abide by the Eligible User's drug-free workplace policies when it is accessing Non-Public Data or while on the Eligible User's or the State of Utah's premises.

9. **CODE OF CONDUCT:** If Contractor is working at facilities controlled or owned by the State of Utah, Contractor shall follow and enforce the agency applicable code of conduct. Contractor will ensure that each employee receives a copy of the policies and applicable codes of conduct. (DTS Policy 2000-0001 Code of Conduct, DTS Policy 1000-0003 Acceptable Use of Information Technology Resources)

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

10. INDEMNITY AND LIABILITY

a. **Indemnity Clause:** Defer to NASPO MA Terms and Conditions.

b. **Governmental Immunity Act:** In accordance with the Constitution of the State of Utah and the Governmental Immunity Act of Utah ("the Act", Utah Code §§ 63G-7-101 to 904, as amended), the Division and the State of Utah have no liability for the operations, acts, or omissions of the Contractor or any third party. Any indemnity obligations of the Division, Eligible Users, or the State of Utah are subject to the Constitution of the State of Utah and the Act and limited to claims that arise from and to the extent caused by the negligent acts or omissions of the Division or the Eligible Users in the performance of the Division's or the Eligible User's obligations under this Contract.

c. **Intellectual Property Indemnification:** Contractor warrants and represents it has full ownership and clear title free of all liens and encumbrances to any Good delivered under this contract. Contractor also warrants that any Good, Custom Deliverable, or Service furnished by Contractor under this Contract, including its use by the Eligible Users in unaltered form, will not infringe any copyrights, patents, trade secrets, or other proprietary rights.

Contractor will release, indemnify, and hold the Division, the Eligible Users, and the State of Utah harmless from liability or damages of any kind or nature, including Contractor's use of any copyrighted or un-copyrighted composition, secret process, patented or un-patented invention, article, or appliance furnished or used in Contractor's performance of this Contract. Additionally, if such a claim or liability is based upon an allegation that a Good, Custom Deliverable, or Service furnished by Contractor infringes on any right protected by any patent, copyright, trademark, trade secret, and/or proprietary right, Contractor shall indemnify and hold harmless the Division, the Eligible Users, and the State of Utah for any judgments, settlements, costs, and reasonable attorneys' fees resulting from such a claim or liability. Contractor shall defend all actions brought upon such matters to be indemnified hereunder and pay all costs and expenses incidental thereto; however, the Eligible Users shall have the right, at its option, to participate in the defense of any such action at its own expense without relieving Contractor of any obligation hereunder. If there are any limitations of liability in this Contract, such limitations will not apply to this section. (UCA § 63G-6a-1203(4))

11. HARDWARE WARRANTY: THE STATE OF UTAH DOES NOT ACCEPT ANY PROCUREMENT ITEM "AS-IS". Defer to NASPO MA Warranty Terms and Conditions.

12. SOFTWARE WARRANTY: THE STATE OF UTAH DOES NOT ACCEPT ANY PROCUREMENT ITEM "AS-IS". CONTRACTOR WARRANTS FOR A PERIOD OF **NINETY DAYS** FROM THE DATE OF ACCEPTANCE THAT THE SOFTWARE PORTIONS OF THE GOODS AND CUSTOM DELIVERABLES THAT CONTRACTOR DIRECTLY OR INDIRECTLY PROVIDES WILL: (A) PERFORM IN ACCORDANCE WITH THE SPECIFIC CLAIMS PROVIDED IN THE RESPONSE; (B) BE SUITABLE FOR THE ORDINARY PURPOSES FOR WHICH SUCH GOODS AND CUSTOM DELIVERABLES ARE USED; (C) BE SUITABLE FOR ANY SPECIAL PURPOSES THAT THE ELIGIBLE USER HAS RELIED ON CONTRACTOR'S SKILL OR JUDGMENT TO CONSIDER WHEN IT ADVISED THE STATE ABOUT THE GOODS OR CUSTOM DELIVERABLES; (D) HAVE BEEN PROPERLY DESIGNED AND MANUFACTURED; AND (E) BE FREE OF SIGNIFICANT DEFECTS. CONTRACTOR SHALL PROVIDE THE ELIGIBLE USER WITH BUG FIXES, INCLUDING INFORMING THE ELIGIBLE USERS OF ANY KNOWN SOFTWARE BUGS OR SOFTWARE DEFECTS THAT MAY AFFECT THE STATE'S USE OF THE SOFTWARE. PRODUCT LIABILITYY DISCLAIMERS AND/OR WARRANTY DISCLAIMERS FROM CONTRACTORS OR ITS SUPPLIERS ARE REJECTED.

13. WARRANTY REMEDIES: Defer to Breach of Warranty NASPO MA Terms and Conditions.

14. UPDATES AND UPGRADES: Any upgrades and updates provided by Contractor are subject to the terms of this Contract. If Software is on premises, the State Entity reserves the right to accept updates and upgrades at its discretion and to determine if such updates comply with the Security requirements in the Contract. Contractor shall keep any applicable hardware, software, middleware, and application plugins up to date and in a state of good repair. All patches, critical vulnerabilities, and/or hardware issues must be addressed based on response times by criticality as laid out in the SOW. If the State hosts the solution, then Contractor may request such maintenance from the DTS hosting team. .

15. BUG FIXING AND REMOTE DIAGNOSTICS: Contractor shall use commercially reasonable efforts to provide work-around solutions or patches to reported software problems. With the Eligible User's prior written authorization, Contractor may perform remote diagnostics to work on reported problems. If the Eligible User declines remote

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

diagnostics, Contractor and the Eligible User may agree to on-site technical support, subject to the terms of the Contract.

16. **TECHNICAL SUPPORT AND MAINTENANCE:** If technical support and maintenance is required by the Contract, Contractor will use commercially reasonable efforts to respond to the Eligible User in a reasonable time, and in all events, in accordance with the specific timeframes detailed in the Contract, when the Eligible User makes technical support or maintenance requests.

17. **PHYSICAL DELIVERY:** Defer to NASPO MA Terms and Conditions but for the following: All deliveries under this Contract will be F.O.B. Destination Freight Prepaid and Allowed, unless specifically negotiated otherwise and explicitly written in this contract, with all transportation and handling charges paid for by Contractor.

18. **ELECTRONIC DELIVERY:** Contractor may electronically deliver any Good or Custom Deliverable to the Eligible User or provide any Good and Custom Deliverable for download from the Internet, if pre-approved in writing by the Eligible User. Contractor shall ensure the confidentiality of electronic deliveries in transit. Contractor warrants that all electronic deliveries will be free of known malware, bugs, Trojan horses, etc.

19. **ACCEPTANCE PERIOD:** A Good, Custom Deliverable, or Service furnished under this Contract shall function in accordance with the specifications identified in this Contract and Solicitation. If the Goods and Custom Deliverables delivered do not conform to the specifications identified in this Contract and Solicitation ("Defects"), the Eligible User shall within thirty (30) calendar days of the delivery date ("Acceptance Period") notify Contractor in writing of the Defects. Upon receiving notice, Contractor shall use reasonable efforts to correct the Defects within fourteen (14) calendar days ("Cure Period"). The Eligible User's acceptance of a Good, Custom Deliverable, or Services occurs at the end of the Acceptance Period or Cure Period, whichever is later.

    If after the Cure Period, a Good, Custom Deliverable, or Service still has Defects, then the Eligible User may, at its option: (a) declare Contractor to be in breach and terminate this Contract; (b) demand replacement conforming Goods, Custom Deliverables, or Services from Contractor at no additional cost to the Eligible User; or (c) continue the Cure Period for an additional time period agreed upon by the Eligible User and Contractor in writing. Contractor shall pay all costs related to the preparation and shipping of the replacement products. No products shall be deemed accepted and no invoices shall be paid until acceptance. The warranty period will begin upon the end of the Acceptance Period.

20. **SECURE PROTECTION AND HANDLING OF STATE DATA:** If Contractor is given access to State Data, the protection of State Data shall be an integral part of the business activities of Contractor, and Contractor shall ensure that there is no inappropriate or unauthorized use of State Data. Contractor shall safeguard the confidentiality, integrity, and availability of the State Data and comply with the conditions outlined below. The Eligible User reserves the right to verify Contractor's adherence to the following conditions to ensure they are met:
    a. **Network Security**: Contractor shall maintain network security that, at a minimum, includes: network firewall provisioning, intrusion detection, and regular third-party penetration testing. Contractor shall maintain network security and ensure that Contractor network security policies conform to one of the following:
        1) Current standards set forth and maintained by the National Institute of Standards and Technology, includes those at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.pdf; or
        2) Contractor shall comply with all applicable FedRAMP or GovRAMP security requirements, including but not limited to, continuous monitoring, incident response, and data classification as outlined in GovRAMP documentation.
    b. **State Data Security:** Contractor shall protect and maintain the security of State Data with protection that is at least as good as or better than that maintained by the State of Utah which will be provided by an Eligible User upon Contractor's request (*DTS Policy 5000-0002*). These security measures included but are not limited to maintaining secure environments that are patched and up to date with all appropriate security updates as designated (ex. Microsoft Notification). Data access must incorporate the principles of test privilege and be physically and technologically controlled. The Eligible User reserves the right to determine if Contractor's level of protection meets the Eligible User's security requirements.
    c. **State Data Transmission**: Contractor shall ensure all transmission or exchange of system application data with the Eligible User and State of Utah and/or any other parties expressly designated by the State of Utah, shall be encrypted and take place via secure means (ex. HTTPS or FTPS). Transmission of regulatory data must conform with the current regulatory requirement applicable to such data (ex. FIPS 140-x).

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

d. **State Data Storage**: All State Data will be stored and maintained in data centers in the United States. State Data is required to be encrypted in transit and at rest. State Data may only be processed on or transferred to Contractor-owned portable or laptop computing device or portable storage medium if such device is whole disk encrypted, or used and kept only at Contractor's United States data centers, including if such medium is part of the Contractor's designated backup and recovery process. IN NO CASE MAY SUCH DEVICES OR STATE DATA LEAVE THE UNITED STATES.

e. **Access**: Contractor shall permit its employees and Subcontractors to remotely access non-State Data only as required to provide technical support.

f. **State Data Encryption**: Contractor shall store all data provided to Contractor, including State, as well as any backups made of that data, in encrypted form based on the current TLS standard and include all data as part of a designated backup and recovery process. Encryption of regulatory data must conform with the current regulatory requirement applicable to such data (ex. FIPS 140-x).

g. **Authentication**: Any portable or laptop computer that has access to the Eligible User's or State of Utah resources, or stores any Eligible User data shall be equipped with strong and secure password protection. All systems that require authentication must use the Single Sign On solution operated by the State of Utah. This may be accomplished through federation using standard authentication protocols or direct integration into the vendor supplied application. If the Goods or Services, or both, are to be accessed or used by both Internal (state employees, contractors, etc.) and External (public, etc.) users, then the Goods and Services must be able to be integrated with multiple identity providers at the same time.

h. **Confidential Information Certification:** Contractor may be required to sign a Confidential Information Certification form prior to being given access to confidential computerized records if required by Eligible Users or Federal policies..

i. **State Data Re-Use:** All data exchanged shall be used expressly and solely for the purpose enumerated in this Contract. No State Data of any kind may be transmitted, exchanged, or provided to other contractors or third parties except on a case-by-case basis as specifically agreed to in writing by the Eligible User.

j. **State Data Destruction**: No sooner than 60 days but no later than 90 days following the expiration or termination of this Contract, and only after ensuring compliance with Section 32 (Ownership, Protection, and Return of Documents and Data) of this Attachment A, Contractor shall erase, destroy, and render unreadable all State Data from all non-state computer systems and backups, and certify in writing that these actions have been completed within thirty (30) days of the expiration or termination of this Contract or within seven (7) days of the request of the Eligible User, whichever shall come first, unless the Eligible User provides Contractor with a written directive. The Eligible User's written directive may require that certain data be preserved in accordance with applicable law.

k. **Services Shall Be Performed Within the United States**: All Non-Public Data, including Criminal Justice Information (CJI), Personally Identifiable Information (PII), and other sensitive data, must be stored, processed, and disposed of within the United States. Contractor is prohibited from transferring, storing, or accessing Non-Public and/or State Data outside the United States without explicit written authorization from the State of Utah via an approved exception request from the Chief Information Security Officer (CISO) and must be documented in the system security plans of such systems, with a description of any compensating controls and a business justification. Offshore support is only permitted for systems not using Non-Public Data. Contractor must provide a list of countries and Subcontractors from which Services will be provided to ensure no undue risk to State Data and systems.

l. **Federal Data Protection**: Contractor shall store all Federal Data in a manner that, at all times, is physically and electronically secure from access by unauthorized persons. Contractor shall employ both physical and technological barriers to prevent unauthorized retrieval of Federal Data via computer, remote terminal, or other means. Federal Data must be subject to separation-of-duties protocols and provided only to those with a need to know.

    1) Contractor shall store each query for Federal Data in Contractor's system (including read-only and system access events that do not result in a change to data or a new transaction) as a separate record, not overlaid by subsequent records. All viewing of Federal Data must be recorded by a fully-automated audit trail system, which can be via an online query, automated report, batch processing, or any other logical means. Access to the audit file must be restricted to authorized users with a need to know and be

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

maintained for a minimum of three years or the amount of time required by a federal agency, whichever is greater.

2) Contractor shall delete, purge, destroy, or return to the State of Utah all Federal Data upon termination of the Contract with no output retained by Contractor. If immediate purging is not possible, Contractor shall certify that any Federal Data in physical or electronic storage will remain safeguarded to prevent unauthorized disclosure. Contractor agrees to abide by all relevant federal laws, restrictions on access, use, disclosure, and security requirements in the State's data exchange agreement with the social security administration, including receipt of security awareness training by Contractor's employees who have access to Federal Data through this Contract. Contractor shall permit the State to conduct, at least once every three years and upon prior notice, a review to verify that the Contract is in compliance with the State's agreement with the social security administration.

3) Federal Data may be used only for the purpose of carrying out the provisions of the Contract. Federal Data must be treated as confidential and may not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract.

4) All computer systems receiving, processing, storing, or transmitting Federal Data must meet the requirements set forth by the applicable federal agency

21. **SECURITY INCIDENT OR DATA BREACH NOTIFICATION:** As required by Utah Code 63A-19-405 or any other applicable data breach reporting laws, upon discovery of any Security Incident or Data Breach or privacy breach of Personal Data (including loss of access to Personal Data), Contractor shall provide the notification to the State Entity and DTS in the most expedient time possible without unreasonable delay. Contractor shall adhere to all applicable data breach reporting laws and will, upon the State of Utah's request, provide Contractor's incident response plans to the State of Utah. It is within the Eligible User's discretion to determine whether any attempted unauthorized access is a Security Incident or a Data Breach.

    a. **Incident Response**: Contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement and seeking external expertise as mutually agreed upon, defined by law or contained in this Contract. Discussing Security Incidents with the Eligible User should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes, defined by law or contained in this Contract.

    b. **Security Incident Reporting Requirements**: Contractor shall promptly report a Security Incident to the Eligible User. In the event Eligible User is a State of Utah Entity, contact should be made as follows:

        Email – DTS-SOC@utah.gov

        Phone – (801) 538-3011

        Web – cybercenter@utah.gov

22. **LIABILITY FOR SECURITY INCIDENT OR DATA BREACH.** In the event of a Security Incident or Data Breach, liability for notification, remedial costs, and damages shall be the responsibility of the party who controls how the data is processed.

23. **SECURITY INCIDENT OR DATA BREACH RESPONSIBILITIES:** Contractor shall comply with all applicable laws that require the notification of individuals in the event of a Security Incident or Data Breach or other events requiring notification (*DTS Policy 5000-0002 Enterprise Information Security Policy)*. In the event of a Security Incident or Data Breach or other event requiring notification under applicable law (UCA § 63a-19-405 and 406), Contractor shall: (a) cooperate with the Eligible User by sharing information relevant to the Security Incident or Data Breach; (b) promptly implement necessary remedial measures, if necessary; and (c) document responsive actions taken related to the Security Incident or Data Breach, including any post-incident review of events and actions taken to make changes in business practices in relation to the Security Incident or Data Breach. If the Security Incident or Data Breach requires public notification, all communication shall be coordinated with the Eligible User. Contractor is responsible for all notification and remedial costs and damages.

24. **STATE INFORMATION TECHNOLOGY POLICIES:** If Contractor is providing an Executive Branch Agency of the State of Utah with Goods or Custom Deliverables, Contractor shall comply with policies and procedures that meet or exceed those DTS follows for internally developed goods and deliverables to minimize security risk, ensure

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

applicable Utah and Federal laws are followed, address issues with accessibility and mobile device access, and prevent outages and data breaches within the State of Utah's environment. Contractor shall comply with the following DTS Policies:

a. **DTS Policy 4000-0001, Enterprise Application and Database Deployment Policy**: A Contractor developing software for the State to develop and establish proper controls that will ensure a clear separation of duties between developing and deploying applications and databases to minimize security risk; to meet due diligence requirements pursuant to applicable Utah and federal regulations; to enforce contractual obligations; and to protect the State's electronic information and information technology assets.

b. **DTS policy 4000-0002, Enterprise Password Standards Policy**: A Contractor developing software for the State must ensure it complies with the password requirements of the Enterprise Password Standards Policy.

c. **DTS Policy 4000-0003, Software Development Life Cycle Policy**: A Contractor developing software for the State shall work with DTS in implementing a Software Development Lifecycle (SDLC) that addresses key issues of security, accessibility, mobile device access, and standards compliance.

d. **DTS Policy 4000-0004, Change Management Policy**: Goods or Custom Deliverables furnished or Services performed by Contractor which have the potential to cause any form of outage or to modify DTS's or the State of Utah's infrastructure must be reviewed by the DTS Change Management Committee. Any outages or Data Breaches which are a result of Contractor's failure to comply with DTS instructions and policies will result in Contractor's liability for all damages resulting from or associated with the outage or Data Breach.

e. **Applicability of DTS Policies:** When a new product or service is added by the Contractor or a reseller, that product or service must be subject to, and comply with, the latest version of these DTS policies, which will be provided upon Contractor's request by the Division of Technology Services.

25. CONFIDENTIALITY: If Contractor has access to or processes Confidential Information, Contractor shall: (i) advise its agents, officers, employees, partners, and Subcontractors of the obligations set forth in this Contract; (ii)keep all Confidential Information strictly confidential; and (iii) comply with any requirements contained in the contract regarding permitted uses and disclosures of personal data, measures designed to safeguard personal data, and the destruction of personal data. Contractor will promptly notify the State Entity of any potential or actual misuse or misappropriation of Confidential Information, including any data breaches, in accordance with UCA 63A-19 Government Data Privacy Act. In Accordance with UCA 63A-19, Contractor must comply with all the same requirements regarding personal data as the State.

Contractor shall be responsible for any breach of this duty of confidentiality, including any required remedies and/or notifications under applicable law. Contractor shall indemnify, hold harmless, and defend the Eligible User, including anyone for whom the Eligible User is liable, from claims related to a breach of this duty of confidentiality, including any notification requirements, by Contractor or anyone for whom the Contractor is liable.

If Contractor's Subcontractors have access to or process Personal Data, Contractor shall advise the Subcontractor of the obligations required under this Contract to keep all Personal Data strictly confidential and advise the Subcontractor to comply with any requirements contained in the Contract such as permitted uses, disclosures, handling, and destruction of Personal Data. Some privacy and data protection laws may require disclosure of Subcontractors who process State Data that includes Personal Data.

Upon termination or expiration of this Contract, Contractor will return all copies of Confidential Information to the Eligible User or certify, in writing, that the Confidential Information has been destroyed. This duty of confidentiality shall be ongoing and survive the termination or expiration of this Contract.

26. Reserved

27. OWNERSHIP IN INTELLECTUAL PROPERTY: The Parties recognize that each has no right, title, or interest, proprietary or otherwise, in or to the name, logo, or intellectual property owned or licensed by the other. The Parties shall not, without the prior written consent of the other or as authorized in this Contract, use the name, logo, or intellectual property owned or licensed by the other.

28. OWNERSHIP IN CUSTOM DELIVERABLES: Contractor warrants, represents and conveys full ownership, clear title free of all liens and encumbrances to any Custom Deliverable. Contractor conveys the ownership in Custom Deliverables as defined in this Attachment A to the Eligible User. All intellectual property rights, title and interest in the Custom Deliverables shall transfer to the Eligible User, subject to the following:

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

a. Contractor has received payment for the Custom Deliverables,

b. Each party will retain all rights to Background IP, even if embedded in the Custom Deliverables.

c. Custom Deliverables, excluding Contractor's Background IP may not be marketed or distributed without written approval by the Eligible User.

Contractor shall grant to the Eligible User a perpetual, irrevocable, royalty-free license to use Contractor's Background IP as defined above, solely for the Eligible User to use the Custom Deliverables.

29. **LICENSE FOR GOODS:** For any software, including SaaS, delivered that is not considered a Custom Deliverable, Contractor grants the Eligible User a non-exclusive, non-transferable, right to use, without the right to sublicense, such software for the Eligible Users internal business operation under this Contract. If the software is perpetual, Contractor grants the Eligible User a non-exclusive, non-transferable, irrevocable, perpetual right to use and copy, without the right to sublicense, for DTS's and the Eligible Users internal business operation under this Contract.

30. **OWNERSHIP, PROTECTION, AND USE OF RECORDS:** The Eligible User shall own exclusive title to all information and data gathered, reports developed, and conclusions reached by the Eligible User in performance of this Contract. Contractor may not use, except in meeting its obligations under this Contract, information gathered, reports developed, or conclusions reached by the Eligible User in performance of this Contract without the express written consent of the Eligible User. This includes information in anonymized or aggregated formats.

31. **OWNERSHIP, PROTECTION, AND USE OF DATA:** The Eligible User shall own and retain unlimited rights to use, disclose, or duplicate all information and data (copyrighted or otherwise) developed, derived, documented, stored, or furnished by Contractor under this Contract. Contractor, and any Subcontractors under its control, expressly agrees not to use Non-Public Data without prior written permission from the Eligible User.

32. **OWNERSHIP, PROTECTION, AND USE OF CONFIDENTIAL FEDERAL, UTAH, OR LOCAL GOVERNMENT INTERNAL BUSINESS PROCESSES AND PROCEDURES:** In the event that the Eligible User provides Contractor with confidential federal or state business processes, policies, procedures, or practices, pursuant to this Contract, Contractor shall hold such information in confidence, in accordance with applicable laws and industry standards of confidentiality, and not to copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of, give, or disclose such information to third parties or use such information for any purpose whatsoever other than the performance of this Contract. The improper use or disclosure by any party of protected internal federal or state business processes, policies, procedures, or practices is prohibited. Confidential federal or state business processes, policies, procedures, or practices shall not be divulged by Contractor or its Subcontractors, except for the performance of this Contract, unless prior written consent has been obtained in advance from the Eligible User.

33. **OWNERSHIP, PROTECTION, AND RETURN OF DOCUMENTS AND DATA UPON CONTRACT TERMINATION OR COMPLETION:** All documents and data pertaining to work required by this Contract will be the property of the Eligible User, and must be delivered to the Eligible User upon its request at any time during the Contract Period, as well as within thirty (30) working days after termination or expiration of this Contract, and without restriction or limitation to their future use. Any State Data returned under this section must either be in the format as originally provided, in a format that is readily usable by the Eligible User, or formatted in a way that it can be used. The Contractor shall pay the costs for returning documents and data to the Eligible User except as specified in this Contract.

34. **ORDERING AND INVOICING:** All orders will be shipped promptly in accordance with the delivery schedule. Contractor will promptly submit invoices (within 30 days after shipment or delivery of goods or services, with the exclusion of end of fiscal year invoicing for Executive Branch Agencies) to the appropriate Eligible User. The contract number shall be listed on all invoices, freight tickets, and correspondence relating to an order under this Contract. The prices paid by the Eligible User shall not exceed prices listed in this Contract. The Eligible User shall adjust or return any invoice reflecting incorrect pricing. For Executive Branch Agencies, Contractor must send all invoices no later than July 10, or the last working day prior, to the State for all work completed or items received during the State's fiscal year of July 1-June 30.

35. **PAYMENT AND NOTICE:**

a. Payments will be made within thirty (30) days from the date a correct invoice is received. For Executive Branch Agencies, a correct invoice will contain the contract and purchase order numbers as indicated in Section 33. After sixty (60) days from the date a correct invoice is received by the appropriate State official, the Contractor may assess interest on overdue, undisputed account charges up to the interest rate paid by the IRS on refund

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

claims, plus two percent, computed in accordance with UCA § 15-6-3, Utah Prompt Payment Act of Utah Code, as amended.

b. The contract costs may be changed only by written amendment. All payments to Contractor will be remitted by mail, by electronic funds transfer, or by the Eligible User's purchasing card (major credit card). Eligible Users will not pay electronic payment fees of any kind.

c. Any written protest of the final contract payment must filed with the Eligible User within ten (10) working days of receipt of final payment. If no protest is received, the Eligible User, the Division, and the State of Utah are released from all claims and all liability to Contractor for fees and costs pursuant to this Contract.

d. Overpayment: If during or subsequent to the Contract an audit determines that payments were incorrectly reported or paid by the Eligible User to Contractor, then Contractor shall, upon written request, immediately refund to the Eligible User any such overpayments.

36. CONTRACTOR'S INSURANCE RESPONSIBILITY: Defer to NASPO MA Terms and Conditions for insurance coverage types and amounts.

Certificate of Insurance, showing up-to-date coverage, shall be on file with the State before the Contract may commence. Failure to provide proof of insurance as required will be deemed a material breach of this Contract. Contractor shall add the State of Utah as an additional insured with notice of cancellation. Contractor's failure to maintain this insurance requirement for the Contract Period will be grounds for immediate termination. (UCA § 63G-6a-1203)

37. ASSIGNMENT/SUBCONTRACT: Contractor will not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Contract, in whole or in part, without the prior written approval of the Division.

38. TERMINATION: Defer to NASPO MA Terms and Conditions but for the following: If the Contractor cannot certify the statement contained in the NASPO MA Terms and Conditions, attach a written explanation for review by the Lead State.

39. TERMINATION UPON DEFAULT: In the event this Contract is terminated for default by Contractor, the Division may procure Goods, Custom Deliverables, or Services similar to those terminated, and Contractor shall be liable to the Division for any and all cover costs and damages.

40. SUSPENSION OF WORK: The Division may suspend Contractor's responsibilities under this Contract without terminating this Contract by issuing a written notice. Contractor's responsibilities may then be reinstated upon written notice from the Division.

41. DEFAULT AND REMEDIES: Any of the following events will constitute cause for the Division to declare Contractor in default of this Contract for nonperformance of contractual requirements or a material breach of any term or condition of this Contract. The Division will issue a written notice of default and may provide a fourteen (14) day period in which Contractor will have an opportunity to cure. Time allowed for cure will not diminish or eliminate Contractor's liability for damages. If the default remains, after Contractor has been provided the opportunity to cure, the Division may exercise any remedy provided by law; terminate this Contract and any related contracts or portions thereof; (c) impose liquidated damages, if liquidated damages are listed in the contract; (d) suspend or debar Contractor from receiving future solicitations; or (e) demand a full refund of the Goods, Custom Deliverables, or Services furnished by Contractor that are defective or Services that were inadequately performed.

42. FORCE MAJEURE: Neither party to this Contract will be held responsible for delay or default caused by fire, riot, acts of God, or war which is beyond that party's reasonable control. The Division may immediately terminate this Contract after determining such delay will reasonably prevent successful performance of this Contract.

43. CONFLICT OF TERMS: Contractor terms and conditions must be attached to this Contract. No other terms and conditions will apply to this Contract, including terms listed or referenced on a Contractor's website, quotation/sales order, purchase orders, or invoice. In the event of any conflict in the contract terms and conditions, defer to the order of precedence in the NASPO MA.

44. SURVIVORSHIP: The contractual provisions that will remain in effect after expiration or termination of this Contract are: (a) Contract Jurisdiction, Choice of Law, and Venue; (b) Secure Protection and Handling of State Data; (c) Data Breach Responsibilities; (d) Ownership in Custom Deliverables; (e) Ownership, Protection, and Use of Records, including Residuals of such records; and (f) Ownership, Protection, and Use of Confidential Federal, Utah, or Local Government Internal Business Processes, including residuals of such confidential business

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

processes; (g) Ownership, Protection, and Return of Documents and Data Upon Contract Termination or Completion; (h) Confidentiality; (i) Conflict of Terms; and (j) any other terms that by their nature would survive the expiration, completion, or termination of this contract.

45. RELEVANT STATE AND FEDERAL LAWS

a. **Conflict of Interest with State Employees:** Contractor shall comply and cooperate in good faith with all conflict of interest and ethic laws, including UCA § 63G-6a-2404, Utah Procurement Code, as amended.

b. **Procurement Ethics:** Contractor understands that a person who is interested in any way in the sale of any supplies, services, products, construction, or insurance to the State of Utah is violating the law if the person gives or offers to give any compensation, gratuity, contribution, loan, or reward, or any promise thereof to any person acting as a procurement officer on behalf of the State of Utah, or who in any official capacity participates in the procurement of such supplies, services, products, construction, or insurance, whether it is given for their own use or for the use or benefit of any other person or organization (UCA § 63G-6a-2404, Utah Procurement Code, as amended).

c. **Contact Information:** Per UCA §§ 63G-6a-110 and 35A-2-203, the State shall make Contractor's contact information available to the State of Utah Department of Workforce Services. The State of Utah Department of Workforce Services may post information regarding Contractor's job vacancies on its website.

d. **Employment Practices:** Contractor shall abide by the following employment laws: (i)Title VI and VII of the Civil Rights Act of 1964 (42 U.S.C. 2000e) which prohibits discrimination against any employee or applicant for employment or any applicant or recipient of services, on the basis of race, religion, color, or national origin; (ii) Executive Order No. 14173 (iii) 45 CFR 90 which prohibits discrimination on the basis of age; (iv) Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act of 1990 which prohibits discrimination on the basis of disabilities; and (v) Utah's Executive Order 2019-1, dated February 5, 2019, which prohibits unlawful harassment in the work place. Contractor shall abide by any other laws, regulations, or orders that prohibit the discrimination of any kind of any of Contractor's employees.

e. **Compliance with Accessibility Standards:** Contractor shall comply with the Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973. Contractor shall comply with Utah Administrative Code R895-14-3(3), which states that contractors developing new websites, hardware or software, for State agencies are required to meet accessibility guidelines subject to rule R895 and correct any items that do not meet these guidelines at no cost to the agency. Contractor shall comply with Utah Administrative Code R895-14-4(2), which states that contractors proposing IT products and services shall provide Voluntary Product Accessibility Template® (VPAT™) documents.

46. RIGHT TO MONITOR PERFORMANCE AND AUDIT

a. **Audit:** Contractor shall, upon written notification permit the Division, or a third party designated by the Division, to perform an assessment, audit, examination, or review of all of Contractor's sites and environments - including physical, technical, and virtual sites and environments - in order to confirm Contractor's compliance with this Contract; associated scopes of work; and applicable laws, regulations, industry standards and applicable GovRAMP requirements. Contractor shall fully cooperate with such assessment by providing access to knowledgeable personnel; physical premises; records; technical and physical infrastructures; and any other person, place, or object which may assist the Division or its designee in completing such assessment. Upon request, Contractor shall provide the results of any audit performed by or on behalf of Contractor that would assist the Division or its designee in confirming Contractor's compliance with this Contract; associated scopes of work; and applicable laws, regulations, industry standards and applicable GovRAMP requirements. If Federal Data is involved, this provision may not be waived to restrict Federal audit requirements.

b. **Monitor Performance**: The Division and Eligible Users reserve the right to monitor Contractor's performance, perform plan checks, plan reviews, other reviews, and/or comment upon the Services of Contractor. This includes Contractor's Subcontractors, if any. Results of any evaluation may be made available to the Contractor upon Contractor's request.

c. **GovRAMP Continuous Monitoring** – The Contractor will be required to grant access to GovRAMP Continuous Monitoring and reporting upon intent to award for a product utilizing a GovRAMP Security Progressing Snapshot, Core, Ready, Provisionally Authorized or Authorized status throughout the life of the contract. The Division reserves the right to request and review all Third-Party Assessment Organization

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

(3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of the contractor's environment. The contractor shall respond to all flaws discovered by providing a mutually agreed upon timeframe to resolve the issue and/or implement a compensating control.

d. **Contract Compliance**: If Contractor's performance involves the payment card industry, Contractor will obtain a third-party PCI compliance report annually and submit the same to the State upon request. In no event shall the PCI compliance report be more than 12 months old at the time it is provided to the Eligible User.

47. **TIME IS OF THE ESSENCE:** The Services shall be completed and Goods and Custom Deliverables delivered by any applicable deadline stated in this Contract. Time is of the essence.

48. **STANDARD OF CARE:** For Services of Contractor which require licenses and certifications, such Services shall be performed in accordance with the standard of care exercised by licensed members of their respective professions having substantial experience providing similar services which similarities include the type, magnitude, and complexity of the Services that are the subject of this Contract.

49. **LARGE VOLUME DISCOUNT PRICING:** Eligible Users may seek to obtain additional volume discount pricing for large orders provided Contractor is willing to offer additional discounts for large volume orders. No amendment to this Contract is necessary for Contractor to offer discount pricing to an Eligible User for large volume purchases.

50. **ELIGIBLE USER PARTICIPATION:** Participation under this Contract by Eligible Users is voluntarily determined by each Eligible User. Contractor agrees to supply each Eligible User with Goods based upon the same terms, conditions and prices of this Contract.

51. **INDIVIDUAL CUSTOMERS:** Each Eligible User that purchases Goods from this Contract will be treated as if they were individual customers. Each Eligible User will be responsible to follow the terms and conditions of this Contract. Contractor agrees that each Eligible User will be responsible for their own charges, fees, and liabilities. Contractor shall apply the charges to each Eligible User individually. The Division is not responsible for any unpaid invoice.

52. **QUANTITY ESTIMATES:** The Division does not guarantee any purchase amount under this Contract. Estimated quantities are for Solicitation purposes only and are not to be construed as a guarantee.

53. **ORDERING:** Orders will be placed by the using Eligible User directly with Contractor. All orders will be shipped promptly in accordance with the terms of this Contract.

54. **REPORTS AND FEES**:

a. **Administrative Fee:** Contractor agrees to provide a quarterly administrative fee to the State in the form of a check, EFT or online payment through the Division's Automated Vendor Usage Management System. Checks will be payable to the "State of Utah Division of Purchasing" and will be sent to State of Utah, Division of Purchasing, Attn: Cooperative Contracts, PO Box 141061, Salt Lake City, UT 84114-1061. The Administrative Fee will be the amount listed on the PA cover page and will apply to all purchases (net of any returns, credits, or adjustments) made under this Contract.

b. **Quarterly Reports:** Contractor agrees to provide a quarterly utilization report, reflecting net sales to the State during the associated fee period. The report will show the dollar volume of purchases by each Eligible User. The quarterly report will be provided in secure electronic format through the Division's Automated Vendor Usage Management System found at: https://statecontracts.utah.gov/Vendor.**Report Schedule:** Quarterly utilization reports shall be made in accordance with the following schedule:

Period End	Reports Due
March 31	April 30
June 30	July 31
September 30	October 31
December 31	January 31

c. **Fee Payment:** After the Division receives the quarterly utilization report it will send Contractor an invoice for the total quarterly administrative fee owed to the Division. Contractor shall pay the quarterly administrative fee within thirty (30) days from receipt of invoice.

55. **Timely Reports and Fees:** If the quarterly administrative fee is not paid by thirty (30) days of receipt of invoice or

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

quarterly utilization reports are not received by the report due date, then Contractor will be in material breach of this Contract.

56. ANTI-BOYCOTT ACTIONS: In accordance with Utah Code 63G-27 et seq., Contractor certifies that it is not currently engaged in any "economic boycott" nor a "boycott of the State of Israel" as those terms are defined in Section 102. Contractor further certifies that it has read and understands 63G-27 et. seq., that it will not engage in any such boycott action during the term of this Contract, and that if it does, it shall promptly notify the State in writing.

57. END USER AGREEMENTS: If Eligible Users are required by Contractor to sign an End User Agreement before participating in this Contract, then a copy of the End User Agreement must be attached to this Contract as an attachment. An End User Agreement must reference this Contract, and may not be amended or changed unless approved in writing by the Division. Eligible Users will not be responsible or obligated for any early termination fees if the End User Agreement terminates as a result of completion or termination of this Contract.

58. COMPLIANCE WITH NIST 800.53 If Contractor is developing software for the State or providing Goods or Custom Deliverables or performing Services which have the potential to cause any form of outage or to modify any State of Utah infrastructure, Contractor shall comply with current standards set forth and maintained by the National Institute of Standards and Technology, NIST 800-53 (Rev 5 or current version. For cloud solutions, Contractor shall comply with either FedRAMP or GovRAMP requirements at a Public Control Baseline of (Low, Moderate, or High), as determined by DTS or other Eligible User.All cloud service products that process, store, transmit and/or could impact government data must either be FedRAMP authorized or enrolled in the GovRAMP Progressing Snapshot Program or demonstrate compliance with a GovRAMP status (Ready, Provisionally Authorized, or Authorized) with a Public Control Baseline of (Low, Moderate, or High), as defined below. Requirements related to each status are outlined below.

1. **GovRAMP Progressing Security Snapshot Program.** Products without a GovRAMP status of Core, Ready, Authorized, or Provisionally Authorized, must enroll in the GovRAMP Progressing Security Snapshot Program at the time a purchase is made, complete quarterly Snapshots, and provide monthly progress reporting to GovRAMP until GovRAMP Core, GovRAMP Ready, GovRAMP Provisionally Authorized, or GovRAMP Authorized status is obtained. Where required, a product must achieve GovRAMP Core no later than 12 months after a purchase is made and achieve a verified status of GovRAMP Moderate Authorized no later than 24 months after a purchase is made. All products with a purchase order after July 1, 2027 must already have the required GovRAMP status at time the purchase is made. . Subsequent Security Snapshots should reflect progress toward increased security controls and GovRAMP status. Government must be granted visibility and access through GovRAMP for continuous monitoring as requested.

2. **GovRAMP Core.** Products with a GovRAMP Core status must maintain GovRAMP Core status for the duration of the contract, unless a higher status is required by DTS or Eligible User. Government must be granted visibility and access through GovRAMP for continuous monitoring as requested.

3. **GovRAMP Ready.** Products with GovRAMP Ready status must maintain GovRAMP Ready status for the duration of the contract. Government must be granted visibility and access through GovRAMP for continuous monitoring as requested.

4. **GovRAMP Authorized and GovRAMP Provisionally Authorized.** Products with GovRAMP Authorized or GovRAMP Provisionally Authorized status must maintain either a GovRAMP Authorized status or a GovRAMP Provisionally Authorized status for the duration of the contract. Government must be granted visibility and access through GovRAMP for continuous monitoring as requested.

5. **For Eligible Users that fall under the authority of DTS**, any cloud solution that processes, stores, transmits and/or impacts government data that is considered public data (anything that is not included in Non-Public Data) must comply with the DTS Policy 5000-0002 Enterprise Information Security Policy. Contractor is required to ensure that anything quoted to these entities follows this requirement

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

and that if the requested product does not meet these requirements that it is clearly communicated to the requesting entity.

If the contractor fails to maintain or achieve the security requirements outlined above, the Contractor may be subject to liquidated damages and/or the Division may reevaluate the terms of the contract and determine whether the failure to comply justifies contract termination.

59. **USE OF AI OR STATE SUB DOMAIN:** Contractor must inform the Eligible Users of any Generative Artificial Intelligence ("GenAI") in the Goods or Services being contracted for prior to providing those Goods or Services to the State. Additionally, Utilization of generative AI in the creation of Goods and Services impacting the State's Intellectual Property Rights shall include annotations sufficient to comply with DTS POLICY 4000-0008 Enterprise Generative AI Policy.

    a. Contractor is prohibited from using Eligible Users materials or data in generative AI queries without prior written permission from the Eligible User, as well as from building or training proprietary generative AI programs. Contractor attests that its AI models use only properly licensed material. Should Contract be found in violation of this requirement, Contractor shall fully indemnify and defend Eligible Users from all claims related thereto. Furthermore, should Contractor learn that Eligible Users materials or Data has been used in generative AI queries without permission from the Eligible User, Contractor shall immediately notify the Eligible Users of the use and cover the full expense of any remediation.

    b. Contractor shall support usage of a utah.gov subdomain according to R895-4 for Goods and Services that will be made available to non-state users.

    c. Contractor is prohibited from using, integrating, or otherwise conjoining Personal Data with GenAI in any way and under any circumstances.

60. **PUBLICITY and WEBSITE BRANDING:** Contractor shall submit to the Division for written approval all advertising and publicity matters relating to this Contract. Contractor shall only use the approved executive branch agency, and/or State of Utah logo on websites produced under terms of this Contract. It is within the Division's sole discretion whether to provide approval, which approval must be in writing

61. **DEVELOPMENT, TEST, AND PRODUCTION ENVIRONMENTS:** If Goods or Services under this Contract are Contractor-hosted, the Contractor shall include three environments throughout the term of the Contract: a development, test, and production environment. Regular refreshes to the database or application or both will be requested. To perform an application refresh, all developers involved in the project, whether from the Contractor or the State, will need to approve in writing the refresh request to prevent any code from being deleted without a prior backup. The cost to configure and maintain these environments is included in the Contract price and will not be charged beyond the amount noted on the Contract Cover Page.

    a. If a development or test region is promoted to production, that region must have all of the required security and privacy controls and audit requirements prior to promotion.

    b. If the application cannot perform a production refresh after the application is live, then a secondary environment for testing must be created by Contractor.

    c. If the Contractor chooses not to provide the three separate environments required then Contractor shall configure the production environment with dummy or test accounts that have the ability to go through the full application process without causing or creating data or cost discrepancies. Additionally, a device or mechanism, such as a feature flag/banner announcement to call out new features to the user, or canary releases to allow for gradual release to smaller sets of users, must be included. Logging must be enabled in order to identify and diagnose issues and to fulfill audit and regulatory requirements, including security frameworks such as NIST and OWASP. A/B testing, automated testing, and incremental rollouts must also be considered and clarified in lettered additions to this Section 16 (e.g. "d," "e," etc.). A way of communicating upcoming changes via notification, alerts, emails, and updates must be available. Contractor shall make clearly defined fallback strategies and rollback plans available prior to any code promotion

62. **TRANSITION ASSISTANCE:** Upon termination or expiration of the Contract, Contractor shall reasonably cooperate with other parties in connection with all Goods and Services to be delivered, including any successor contractor to whom data is transferred. The Contractor shall assist the Eligible User in exporting and extracting data, in a format usable without the use of the Procurement Item and as agreed to between the

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

parties, at no additional cost. Any transition service requested by the Eligible User involving knowledge transfer and support beyond that described in this paragraph prior to this sentence may be subject to a statement of work at Contractor's then current rates, agreed upon between the parties and added by amendment to this Contract.

63. **BUSINESS ASSOCIATE AGREEMENT**: If the nature of the parties' interactions is such that PHI will be exchanged, the parties will negotiate a Business Associate Agreement in good faith.

64. **Restricted Foreign Entities and Forced Labor:** In accordance with Utah law, Contractors contracting with the State certify that they are not providing a "forced labor product" as defined in Utah Code 63G-6a-121. If the Contractor is providing technology or technology services, networks, or systems, the Contractor certifies that the aforementioned does not come from a "restricted foreign entity," as also defined in UCA 63G-6a-121.

65. No Contractor or third-party terms, including standard click through license or website terms or use of privacy policy, shall apply to Eligible Users unless such terms are included in the NASPO MA.

(Cloud PA's - Revision Date: May 1, 2026,)

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

Participating Entity: State of Utah	Contractor: Istonish, Inc.
Signature: DocuSigned by: C38BE9DAC528424...	Signature: Signed by: Annette Quintana 3CF67F4EE834437...
Name: Windy Aphayrath	Name: Annette Quintana
Title: Chief Procurement Officer	Title: CEO
Date: 7/2/2026	Date: 7/2/2026

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment B

Contract # LS5004

STATE OF UTAH COOPERATIVE CONTRACT

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

Istonish		
Name		
5500 Greenwood Plaza Blvd., Suite 130		
Address		
Greenwood Village	CO	80111
City	State	Zip

LEGAL STATUS OF CONTRACTOR
- ☐ Sole Proprietor
- ☐ Non-Profit Corporation
- ☒ For-Profit Corporation
- ☐ Partnership
- ☐ Government Agency

Contact Person Clinton Marsh Phone # 303-498-0245 Email cmarsh@istonish.com
Vendor #VC228030 Commodity Code #92005

2. CONTRACT PORTFOLIO NAME: Cloud and Software Solutions

3. PROCUREMENT: This Contract is entered into as a result of Solicitation #BP24-1.

4. CONTRACT PERIOD: Effective Date: 9/16/2026 Termination Date: 9/15/2036 unless terminated early or extended in accordance with the terms and conditions of this Contract. Renewal options (if any): None.

5. Prompt Payment Discount (if any): None. Price Guarantee Period (if any): Minimum Percentage Discount: Life of the contract
Direct Service Provide Pricing: 1 year.

6. ATTACHMENT A: NASPO ValuePoint Master Agreement Terms and Conditions
ATTACHMENT B: Scope of Work
ATTACHMENT C: Pricing Catalog
ATTACHMENT D: Contractor's Response to Solicitation
ATTACHMENT E: End User Agreements
ATTACHMENT F: 3rd Party Provider Agreement Template
ATTACHMENT G: IRS Publication 1075 Exhibit 7
Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this Contract.
   b. Utah State Procurement Code, Procurement Rules, the Solicitation, and Contractor's response to the Solicitation. Both the solicitation and Contractor's response to the solicitation, while not included as a listed attachment to the Master Agreement above, will both be available on the NASPO website for transparency less any information marked as confidential by the Contractor at the time of submission.

9. Each person signing this Contract represents and warrants that he/she is duly authorized and has legal capacity to execute and deliver this Contract and bind the parties hereto. Each signatory represents and warrants to the other that the execution and delivery of the Contract and the performance of each party's obligation hereunder have been duly authorized and that the Contract is a valid and legal Contract binding on the parties and enforceable in accordance with its terms.
IN WITNESS WHEREOF, the parties sign and cause this Contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 4 above.

CONTRACTOR

Signed by: Annette Quintana 3CF67F4EE834437...
Contractor's Signature

Annette Quintana — Print Name
CEO — Title
11/14/2025 — Date

STATE

DocuSigned by: C38BE9DAC528424...
Director, Division of Purchasing

11/19/2025 — Date

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

ATTACHMENT A

NASPO VALUEPOINT MASTER AGREEMENT TERMS AND CONDITIONS

I. Definitions

1.1 **Contractor** means a party to this Master Agreement, whether a person or entity, that delivers goods or performs services under the terms set forth in this Master Agreement. Contractor also includes its Fulfillment Partners, employees, Subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement. Contractor does not include Third-party Providers.

1.2 **Data** means all information, whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

For a more granular and complete definition of “Data” as it pertains to SaaS, PaaS, and IaaS solutions, see Section A.1 at the end of the NASPO ValuePoint Master Agreement Terms and Conditions.

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

1.4 **Data Categorization** means the systematic process of classifying and organizing Data based on its sensitivity, value, and the level of risk associated with its handling, storage, and transmission. This process involves assessing Data to determine its impact on security, privacy, and compliance requirements. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

1.5 **Data Ownership and Protection** is defined in section A.1 for SaaS, PaaS, and IaaS. On-Prem will be defined on a case by case basis by any Purchasing Entity seeking an on-prem solution.

1.6 **Disabling Code** means computer instructions or programs, subroutines, code, instructions, Data or functions, including but not limited to:

a. Viruses
b. Worms
c. Date bombs or time bombs
d. Programs or code that self-replicate without manual intervention
e. Instructions programmed to activate at a predetermined time or upon a specified event
f. Trojan horses, defined as programs claiming to do a meaningful function but designed for a different function.
g. Any other malicious software or Data that alters, destroys, inhibits, damages, interrupts, interferes with, or hinders the operation of the Purchasing Entity’s software, applications, and/or its end-user processing environment, the system in which it resides, or any other software or Data on such a system or any other system with which it is capable of communicating.

1.7 **Embedded Software** means one or more software applications which permanently reside on a computing device.

1.8 **End User Agreement** means any agreement or additional terms and conditions that Purchasing Entities are required to sign or accept with Contractor, Fulfillment Partner,

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

or Third-party Provider in order to participate in this Master Agreement and/or receive a Product, including an End User License Agreement (EULA), customer agreement, memorandum of understanding, lease agreement, Contractor's order form, terms of use, or any other named document to the same effect. End User Agreements must contain a clear reference to the Master Agreement including the name of the Contractor and Master Agreement number by which the End User Agreement is governed by and operating under. An End User Agreement may only include terms and conditions unique to the Product and Services provided, and not include general terms and conditions already covered by the Master Agreement or applicable Participating Addendum. Specifically, End User Agreements may not contain the following general terms and conditions already covered by the Master Agreement. If any of the following general terms and conditions are included in an End User Agreement and/or other terms and conditions that contradict terms already contained in the Master Agreement or applicable Participating Addendum, such terms will be considered null and void. If any term in an End User Agreement is determined to be null and void, the remaining terms shall remain in place with full force and effect.

a. Indemnity
b. Limitation of Liability
c. Governing Law and Venue
d. Arbitration or Dispute Resolution
e. Force Majeure
f. Ordering
g. Payment (payment schedules and milestones are acceptable)
h. Termination
i. Defaults and Remedies
j. Master Agreement Order of Precedence

1.9 **Hardware** is defined as any physical component that make up a computer, electronic, or IT infrastructure system.

1.10 **High Risk Data** is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("High Impact Data"). This refers to the Data for which the loss of confidentiality, integrity, or availability could have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

1.11 **Infrastructure as a Service (IaaS)** Further defined in section A.1. IaaS as used in this Master Agreement is defined as the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

1.12 **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.

1.13 **Lead State** means the State centrally administering any resulting Master Agreement(s) who is a party to this Master Agreement.

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

1.15 **Master Agreement** means the underlying agreement executed by and between the Lead State, acting in cooperation with NASPO ValuePoint, and the Contractor, as now

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

or hereafter amended.

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

1.17 **NASPO ValuePoint** is a division of the National Association of State Procurement Officials ("NASPO"), a 501(c)(3) corporation. NASPO ValuePoint facilitates administration of the NASPO 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, the District of Columbia, and territories of the United States. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports, as well as other contract administration functions as assigned by the Lead State.

1.18 **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.

1.19 **Order** or **Purchase Order** means any Purchase Order, sales order, contract or other document used by a Purchasing Entity to commit funds in exchange for a Contractor's delivery of one or more Products under this Master Agreement.

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

1.21 **Participating Entity** means a state (as well as the District of Columbia and US territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states properly authorized to enter into a Participating Addendum, that has executed a Participating Addendum.

1.22 **Participating State** means a state that has executed a Participating Addendum or has indicated an intent to execute a Participating Addendum.

1.23 **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. Federal Tax Information (FTI) as defined by the federal government Internal Revenue Service Publication 1075 (as updated, replaced, or amended over time).

1.24 **Platform as a Service (PaaS)** Further defined in section A.1. PaaS as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

configurations

1.25 **Product** or **Products and Services** means any equipment, software (including Embedded Software), documentation, service, or other deliverable supplied or created by the Contractor pursuant to this Master Agreement. The term Product includes goods and services.

1.26 **Protected Health Information** (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual

1.27 **Purchasing Entity** means a state (as well as the District of Columbia and US territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states if authorized by a Participating Addendum, that issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

1.28 **Service Level Agreement** or **SLA** means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2)the amount of time required for notice by the provider to the public jurisdiction of upcoming changes, (3) security notice requirements, (4) timeframes for response to operational problems and failures, (5) description of service quality, (6) identification of roles and responsibilities, () remedies, such as credits, and (8) an explanation of how remedies or credits are calculated and issued.

1.29 **Software as a Service (SaaS)** Further defined in section A.1. SaaS as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings

1.30 **Solicitation** means the Solicitation resulting in this Master Agreement.

1.31 **Subcontractor** includes contractors, manufacturers, distributors, suppliers, or consultants, at any tier, that are under the direct or indirect control or responsibility of Contractor, including a person or entity that is, or will be, providing Product or Products and Services pursuant to this Master Agreement.

II. Term of Master Agreement

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

II.1 **Initial Term.** The initial term of this Master Agreement is for ten (10) years. The Lead State may, prior to execution, adjust the effective date or duration of the initial term or renewal period of any Master Agreement for the purpose of making the Master Agreement coterminous with others.

II.2 **Amendment Limitations.** The terms of this Master Agreement will not be waived, altered, modified, supplemented, or amended in any manner whatsoever without prior written agreement of the Lead State and Contractor.

II.3 **Amendment Term.** The term of the Master Agreement may be amended past the initial term and stated renewal periods for a reasonable period if in the judgment of the Lead State a follow-on competitive procurement will be unavoidably delayed (despite good faith efforts) beyond the planned date of execution of the follow-on master agreement. This subsection will not be deemed to limit the authority of a Lead State under its state law to otherwise negotiate contract extensions.

III. Order of Precedence

III.1 **Order of Precedence.** The following Order of Precedence will apply to any purchase or Order made under this Master Agreement:

III.1.1 A Participating Entity's Participating Addendum ("PA");

III.1.2 The following Master Agreement Attachments: Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions, including A.1, A.2, and A.3 as applicable, Attachment B: Scope of Work, and Attachment C: Pricing Discounts and Schedule;

III.1.3 A Purchase Order, Service Level Agreement, or Statement of Work/specifications issued against the Master Agreement;

III.1.4 The Solicitation or, if separately executed after award, the Lead State's bilateral agreement that integrates applicable provisions;

III.1.5 Attachment D: Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State;

III.1.6 Attachment E: Contractor, Fulfillment Partner, or Third-party Provider's End User Agreement issued against a Participating Addendum. End User Agreements are expected to be negotiated by a Purchasing Entity seeking to utilize the solution at the time a Project is entered into;

III.1.7 Any other Attachments to the Master Agreement not listed above.

III.2 **Conflict.** These documents will be read to be consistent and complementary. Any conflict among these documents will 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.

III.3 **Participating Addenda.** Participating Addenda will not be construed to diminish, modify, or otherwise derogate any provisions in this Master Agreement between the Lead State and Contractor. The term of a Participating Addendum will not exceed the term of this Master Agreement, except when a Participating Entity determines an extension of its Participating Addendum is necessary to avoid a lapse in contract coverage and is permitted by law.

IV. Participants and Scope

IV.1 **Requirement for a Participating Addendum.** Contractor may not deliver Products under this Master Agreement until a Participating Addendum acceptable to the

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Participating Entity and Contractor is executed.

IV.2 Applicability of Master Agreement. 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, subject to Section III. For the purposes 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.

IV.3 Scope of Work Updates. At the discretion of the Lead State, and subject to agreement by the parties, the scope of this Master Agreement may be amended to include or accommodate new or updated models, versions, or technologies related to the objectives and deliverables set forth in the Solicitation.

IV.4 Obligated Entities. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Participating Entities incur no financial obligations on behalf of other Purchasing Entities.

IV.5 Notice of Participating Addendum. Contractor shall email a fully executed PDF copy of each Participating Addendum to pa@naspovaluepoint.org to support documentation of participation and posting in appropriate databases.

IV.6 Participating Entities.

IV.6.1 If not proscribed by law or by the Chief Procurement Official of the state in which the entity is located, an entity may be eligible to execute a Participating Addendum directly with Contractor. Such entities may include:

IV.6.1.1 Political subdivisions, public agencies, and service districts;

IV.6.1.2 Public and private educational institutions, including K-12 public, charter, and private schools; institutions of higher education; and trade schools;

IV.6.1.3 Federally recognized tribes;

IV.6.1.4 Quasi-governmental entities; and

IV.6.1.5 Eligible non-profit organizations.

IV.6.2 Prior to execution of a Participating Addendum with an entity listed above, Contractor shall coordinate with NASPO to confirm the entity's eligibility to execute a Participating Addendum. A determination that an entity is eligible to execute a Participating Addendum is not a determination that procurement authority exists; each entity must ensure it has the requisite procurement authority to execute a Participating Addendum.

IV.7 Prohibition on Resale. Subject to any specific conditions included in the

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Solicitation or Contractor's proposal as accepted by the Lead State, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products purchased under this Master Agreement. Absent any such condition or explicit permission, this limitation does not prohibit: payments by employees of a Purchasing Entity for Products; sales of Products to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities 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.

IV.8 Individual Customers. Except as may otherwise be agreed to by the Purchasing Entity and Contractor, 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 and as the Participating Entity has in the Participating Addendum, 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.

IV.9 Release of Information. Throughout the duration of this Master Agreement, Contractor must secure from the Lead State prior approval for the release of information that pertains to the potential work or activities covered by the Master Agreement. This limitation does not preclude publication about the award of the Master Agreement or marketing activities consistent with any proposed and accepted marketing plan.

IV.10 No Representations. The Contractor shall not make any representations of NASPO ValuePoint, the Lead State, any Participating Entity, or any Purchasing Entity'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.

V. NASPO ValuePoint Provisions

V.1 Applicability. NASPO ValuePoint is not a party to the Master Agreement. The terms set forth in Section V are for the benefit of NASPO ValuePoint as a third-party beneficiary of this Master Agreement.

V.2 Administrative Fees

V.2.1 NASPO ValuePoint Fee. Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than sixty (60) days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee must be submitted quarterly and is based on all sales of Products and Services under the Master Agreement (less any charges for taxes or shipping). The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with a vendor's response to the Lead State's Solicitation.

V.2.2 State Imposed Fees. Some states may require an additional fee be paid by Contractor directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee rate or amount, payment method, and schedule for such reports and payments will be incorporated into the applicable Participating Addendum. Unless agreed to in writing by the state, Contractor may not adjust the Master Agreement pricing to include the state fee for purchases made by Purchasing Entities

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

within the jurisdiction of the state. No such agreement will affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by Purchasing Entities outside the jurisdiction of the state requesting the additional fee.

V.3 NASPO ValuePoint Summary and Detailed Usage Reports

V.3.1 Sales Data Reporting. In accordance with this section, Contractor shall report to NASPO ValuePoint all Orders under this Master Agreement for which Contractor has invoiced the ordering entity or individual, including Orders invoiced to Participating Entity or Purchasing Entity employees for personal use if such use is permitted by this Master Agreement and the applicable Participating Addendum ("Sales Data"). By placing an Order under this Master Agreement, a Purchasing Entity agrees to have their Data (i) included in reports submitted by Contractor to NASPO ValuePoint and (ii) used by NASPO ValuePoint as set forth in this Master Agreement without limitation, unless otherwise requested in writing by the Purchasing Entity and agreed to in writing by NASPO. Timely and complete reporting of Sales Data by Contractor is a material requirement of this Master Agreement. Reporting requirements, including those related to the format, contents, frequency, or delivery of reports, may be updated by NASPO ValuePoint with reasonable notice to Contractor and without amendment to this Master Agreement. NASPO ValuePoint shall have exclusive ownership of any media on which reports are submitted and shall have a perpetual, irrevocable, non-exclusive, royalty free, and transferable right to display, modify, copy, and otherwise use reports, Data, and information provided under this section.

V.3.2 Summary Sales Data. "Summary Sales Data" is Sales Data reported as cumulative totals by state. Contractor shall, using the reporting tool or template provided by NASPO ValuePoint, report Summary Sales Data to NASPO ValuePoint for each calendar quarter no later than thirty (30) days following the end of the quarter. If Contractor has no reportable Sales Data for the quarter, Contractor shall submit a zero-sales report.

V.3.3 Detailed Sales Data. "Detailed Sales Data" is Sales Data that includes for each Order all information required by the Solicitation or by NASPO ValuePoint, including customer information, Order information, and line-item details. Contractor shall, using the reporting tool or template provided by NASPO ValuePoint, report Detailed Sales Data to NASPO ValuePoint for each calendar quarter no later than thirty (30) days following the end of the quarter. Detailed Sales Data shall be reported in the format provided in the Solicitation or provided by NASPO ValuePoint. The total sales volume of reported Detailed Sales Data shall be consistent with the total sales volume of reported Summary Sales Data.

V.3.4 Sales Data Crosswalks. Upon request by NASPO ValuePoint, Contractor shall provide to NASPO ValuePoint tables of customer and Product information and specific attributes thereof for the purpose of standardizing and analyzing reported Sales Data ("Crosswalks"). Customer Crosswalks must include a list of existing and potential Purchasing Entities and identify for each the appropriate customer type as defined by NASPO ValuePoint. Product Crosswalks must include Contractor's part number or SKU for each Product in Offeror's catalog and identify for each the appropriate Master Agreement category (and subcategory, if applicable), manufacturer part number, Product description, eight-digit UNSPSC Class Level commodity code, and (if applicable) EPEAT value and Energy Star rating. Crosswalk requirements and fields may be updated by NASPO ValuePoint

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

with reasonable notice to Contractor and without amendment to this Master Agreement. Contractor shall work in good faith with NASPO ValuePoint to keep Crosswalks updated as Contractor's customer lists and Product catalog change.

V.3.5 Executive Summary. Contractor shall, upon request by NASPO ValuePoint, provide NASPO ValuePoint with an executive summary that includes but is not limited to a list of states with an active Participating Addendum, states with which Contractor is in negotiations, and any Participating Addendum roll-out or implementation activities and issues. NASPO ValuePoint and Contractor will determine the format and content of the executive summary.

V.3.6 Obligation to Act in Good Faith. The parties acknowledge that this Master Agreement and its terms and pricing have been negotiated for the benefit of the parties, NASPO ValuePoint, Participating Entities, and Purchasing Entities. Apart from a Participating Addendum or Order, Contractor shall not intentionally induce a potential Participating Entity or Purchasing Entity to enter into a separate agreement, the pricing and terms of which are derived from this Master Agreement, for the purpose of avoiding compliance with Contractor's obligations under Section V. Nothing in this Section 5.3.6 shall prohibit Contractor from contracting with an entity with substantially similar pricing and terms if such pricing and terms are independently negotiated with the entity or are consistent with pricing and terms ordinarily offered by Contractor to public sector customers.

V.4 NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review

V.4.1 Staff Education. Contractor shall work cooperatively with NASPO ValuePoint personnel. Contractor shall present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the master agreement and Participating Addendum process, and the manner in which eligible entities can participate in the Master Agreement.

V.4.2 Onboarding Plan. Upon request by NASPO ValuePoint, Contractor shall, as Participating Addendums are executed, provide plans to launch the program for the Participating Entity. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the scope and terms of the Master Agreement as available to the Participating Entity and eligible Purchasing Entities.

V.4.3 Annual Contract Performance Review. Contractor shall participate in an annual contract performance review with the Lead State and NASPO ValuePoint, which may at the discretion of the Lead State be held in person and which may include a discussion of marketing action plans, target strategies, marketing materials, Contractor reporting, and timeliness of payment of administration fees.

V.4.4 Use of NASPO ValuePoint Logo. The NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a separate logo use agreement is executed with NASPO ValuePoint.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

V.4.5 **Most Favored Customer.** Contractor shall, within thirty (30) days of their effective date, notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-party contracts or agreements that may affect the promotion of this Master Agreement or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this Master Agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

V.5 NASPO ValuePoint eMarketPlace

V.5.1 The NASPO ValuePoint cooperative provides an eMarketPlace for public entities to access a central online platform to view and/or purchase the goods, services, and solutions available from NASPO ValuePoint's cooperative Master Agreements. This eMarketPlace is provided by NASPO at no additional cost to the Contractor or public entities. Its purpose is to facilitate the connection of public entities with Contractors who meet the requisite needs for a good, service, or solution by that entity through a NASPO ValuePoint Master Agreement.

V.5.2 Contractor shall cooperate in good faith with NASPO, and any third party acting as an agent on behalf of NASPO, to integrate Contractor's industry presence by either an electronic hosted catalog, punchout site, or providing eQuotes through the NASPO eMarketPlace, per the Implementation Timeline as further described below.

V.5.3 Regardless of how Contractor's presence is reflected in the eMarketPlace (*i.e.*, hosted catalog, punchout site, or eQuote), Contractor's listed offerings must be strictly limited to Contractor's awarded contract offerings through the NASPO award. Products and/or services not authorized through the resulting NASPO cooperative contract should not be viewable by NASPO ValuePoint eMarketPlace users. Furthermore, Products and/or Services not authorized through a Participating Addendum should not be viewable by NASPO ValuePoint eMarketPlace users utilizing that Participating Addendum. The accuracy of Contractor's offerings through the eMarketPlace must be maintained by Contractor throughout the duration of the Master Agreement.

V.5.4 Contractor agrees that NASPO controls which Master Agreements appear in the eMarketPlace and that NASPO may elect at any time to remove any of Contractor's offerings from the eMarketPlace.

V.5.5 Contractor is solely responsible for the accuracy, quality, and legality of Contractor's Content on the eMarketPlace. "Content" means all information that is generated, submitted, or maintained by Contractor or otherwise made available by Contractor on the eMarketPlace, including Contractor catalogs. Contractor's Content shall comply with and accurately reflect the terms and pricing of this Master Agreement.

V.5.6 Contractor's use of the eMarketPlace shall comply with the eMarketPlace's Terms of Use.

V.5.7 Contractor is solely responsible for the security and accuracy of transactions facilitated through the eMarketPlace, including the assessment, collection, and remittance of any sales tax.

V.5.8 Lead State reserves the right to approve all pricing, catalogs, and information on the eMarketPlace. This catalog review right is solely for the

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

benefit of the Lead State and Participating Entities, and the review and approval shall not waive the requirement that Products and Services be offered at prices required by the Master Agreement.

V.5.9 NASPO Participating Entities may have their own procurement system, separate from the NASPO eMarketPlace, that enables the use of certain NASPO Master Agreements. In the event one of these entities elects to use this NASPO ValuePoint Master Agreement (available through the eMarketPlace) but publish to their own eMarketPlace, Contractor agrees to work in good faith with the entity and NASPO to implement the catalog.

V.5.10 In the event a Participating Entity has entity-specific catalog requirements set forth in its Participating Addendum (*e.g.*, entity-specific pricing, restrictions in the scope of offerings, etc.), Contractor shall ensure its eMarketPlace Content for that Participating Entity accurately reflects and is compliant with these requirements.

V.5.11 Implementation Timeline: Following the execution of Contractor's Master Agreement, NASPO will provide a written request to Contractor to begin the onboarding process into the eMarketPlace. Contractor shall have fifteen (15) days from receipt of written request to work with NASPO to set up an enablement schedule, at which time the technical documentation for onboarding shall be provided to Contractor. The schedule will include future calls and milestone dates related to test and go live dates.

V.5.11.1 Contractor's NASPO eMarketPlace account with eQuoting functionality shall minimally be established within thirty (30) days following the written request.

V.5.11.2 Contractor shall deliver either a (1) hosted catalog or (2) punchout site, pursuant to the mutually agreed upon enablement schedule.

V.5.11.3 NASPO will work with Contractor to decide which structures between hosted catalog, punchout site, and/or eQuoting as further described below will be provided by Contractor.

V.5.11.3.1 Hosted Catalog. By providing a hosted catalog, Contractor is providing a list of its awarded Products/Services and pricing in an electronic Data file in a format acceptable to NASPO, such as a tab delimited text file. Contractor is solely responsible for ensuring the most up-to-date versions of its Product/Service offerings approved by the Lead State under this Master Agreement are reflected in the eMarketPlace.

V.5.11.3.2 Punchout Site. By providing a punchout site, Contractor is providing its own online catalog, which must be capable of being integrated with the eMarketPlace as a Standard punchout via Commerce eXtensible Markup Language (cXML). Contractor shall validate that its online catalog is up-to-date. The site must also return detailed UNSPSC codes for each line item.

V.5.11.3.3 eQuoting. NASPO will work with Contractor to set up participation and use to provide eQuotes through the NASPO eMarketPlace. This requirement would be in addition to any requirement to provide a hosted catalog or punchout site.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

V.5.12 Hosted catalogs and punchout sites will provide all of the eMarketPlace standard Data elements/information including, but not limited to, the following:

V.5.12.1 The most current pricing, including all applicable administrative fees and/or discounts, as well as the most up-to-date Product/Service offering the Contractor is authorized to provide in accordance with this Master Agreement;

V.5.12.2 A Lead State contract identification number for this Master Agreement;

V.5.12.3 Detailed Product line item descriptions;

V.5.12.4 Pictures illustrating Products, services, or solutions where practicable; and

V.5.12.5 Any additional NASPO, Lead State, or Participating Addendum requirements.

V.6 Cancellation In consultation with NASPO ValuePoint, the Lead State may, in its discretion, cancel the Master Agreement or not exercise an option to renew, when utilization of Contractor's Master Agreement does not warrant further administration of the Master Agreement. The Lead State may also exercise its right to not renew the Master Agreement if the Contractor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. Cancellation based on nonuse or under-utilization will not occur sooner than two years after execution of the Master Agreement. This subsection does not limit the discretionary right of either the Lead State or Contractor to cancel the Master Agreement or terminate for default subject to the terms herein. This subsection also does not limit any right of the Lead State to cancel the Master Agreement under applicable laws.

V.7 Canadian Participation. Subject to the approval of Contractor, any Canadian provincial government or provincially funded entity in Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Quebec, or Saskatchewan, and territorial government or territorial government funded entity in the Northwest Territories, Nunavut, or Yukon, including municipalities, universities, community colleges, school boards, health authorities, housing authorities, agencies, boards, commissions, and crown corporations, may be eligible to use Contractor's Master Agreement.

V.8 Additional Agreement with NASPO. Upon request by NASPO ValuePoint, awarded Contractor shall enter into a direct contractual relationship with NASPO ValuePoint related to Contractor's obligations to NASPO ValuePoint under the terms of the Master Agreement, the terms of which shall be the same or similar (and not less favorable) than the terms set forth in the Master Agreement.

VI. Pricing, Payment & Leasing

VI.1 Pricing. The prices contained in this Master Agreement or offered under this Master Agreement represent the not-to-exceed price to any Purchasing Entity.

VI.1.1 All discounts must be guaranteed for the initial term of the Master Agreement.

VI.1.2 Requests for a discount adjustment must include sufficient documentation supporting the request. Any adjustment or amendment to the Master Agreement will not be effective unless approved in writing by the Lead State.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

VI.1.3 No retroactive adjustments to prices or rates will be allowed.

VI.2 Payment. Unless otherwise agreed upon in a Participating Addendum or Order, Payment after acceptance will be made within thirty (30) days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance, unless a different late payment amount is specified in a Participating Addendum or Order, or otherwise prescribed by applicable law. Payments will be remitted in the manner specified in the Participating Addendum or Order. Payments may be made via a purchasing card with no additional charge.

VI.3 Leasing or Alternative Financing Methods. The procurement and other applicable laws of some Purchasing Entities may permit the use of leasing or alternative financing methods for the acquisition of Products under this Master Agreement. Where the terms and conditions are not otherwise prescribed in an applicable Participating Addendum, the terms and conditions for leasing or alternative financing methods are subject to negotiation between the Contractor and Purchasing Entity.

VII. Ordering

VII.1 Order Numbers. Master Agreement order and Purchase Order numbers must be clearly shown on all acknowledgments, packing slips, invoices, and on all correspondence.

VII.2 Quotes. Purchasing Entities may define entity-specific or project-specific requirements and informally compete the requirement among companies 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 the Purchasing Entity’s rules and policies. The Purchasing Entity may in its sole discretion determine which Master Agreement Contractors should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost, and other factors considered.

VII.3 Applicable Rules. 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.

VII.4 Required Documentation. Contractor shall not begin work without a valid Purchase Order or other appropriate commitment document under the law of the Purchasing Entity.

VII.5 Term of Purchase. Orders may be placed consistent with the terms of this Master Agreement and applicable Participating Addendum during the term of the Master Agreement and Participating Addendum.

VII.5.1 Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or definite performance period past the then-current termination date of this Master Agreement. In the event the term of any such Order placed under this Master Agreement extends past the termination or expiration of this Master Agreement, the terms and conditions of this Master Agreement shall remain in full force and effect as it applies to such Order and will continue in effect for such Order until the term of that Order expires.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

VII.5.2 Notwithstanding the previous, Orders must also comply with the terms of the applicable Participating Addendum, which may further restrict the period during which Orders may be placed or delivered.

VII.5.3 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.

VII.5.4 Notwithstanding the expiration, cancellation or termination of this Master Agreement, Contractor shall 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, cancellation, or termination of this Master Agreement, or in any manner inconsistent with this Master Agreement's terms.

VII.5.5 Orders for any separate indefinite quantity, task order, 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.

VII.5.6 An Order, including a recurring service, maintenance, or software subscription or upcoming renewal, may be canceled before delivery or performance with 30 days advanced written notice provided by the Purchasing Entity. Purchasing Entity will compensate Contractor up to the date of the cancellation notice for expenses incurred, if any. Any order cancellation will not impact the Master Agreement.

VII.6 Order Form Requirements. All Orders pursuant to this Master Agreement, at a minimum, must include:

VII.6.1 The services or supplies being delivered;

VII.6.2 A shipping address and other delivery requirements, if any;

VII.6.3 A billing address;

VII.6.4 Purchasing Entity contact information;

VII.6.5 Pricing consistent with this Master Agreement and applicable Participating Addendum and as may be adjusted by agreement of the Purchasing Entity and Contractor;

VII.6.6 A not-to-exceed total for the Products or Services being ordered; and

VII.6.7 The Master Agreement number or the applicable Participating Addendum number, provided the Participating Addendum references the Master Agreement number.

VII.7 Communication. All communications concerning administration of Orders placed must 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.

VII.8 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.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

VIII. Shipping and Delivery

VIII.1 Shipping Terms. All deliveries will be F.O.B. destination, freight pre-paid, with all transportation and handling charges paid by the Contractor.

VIII.1.1 Notwithstanding the above, responsibility and liability for loss or damage will remain the Contractor's until final inspection and acceptance when responsibility will pass to the Purchasing Entity except as to latent defects, fraud, and Contractor's warranty obligations.

VIII.2 Minimum Shipping. The minimum shipment amount, if any, must be contained in the Master Agreement. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an Order to be shipped without transportation charges that is back ordered will be shipped without charge.

VIII.3 Inside Deliveries. To the extent applicable, all deliveries will be "Inside Deliveries" as designated by a representative of the Purchasing Entity placing the Order. Inside Delivery refers to a delivery to a location other than a loading dock, front lobby, or reception area. Specific delivery instructions will be noted on the order form or Purchase Order. Costs to repair any damage to the building interior (*e.g.*, scratched walls, damage to the freight elevator, etc.) caused by Contractor or Contractor's carrier will be the responsibility of the Contractor. Immediately upon becoming aware of such damage, Contractor shall notify the Purchasing Entity placing the Order.

VIII.4 Packaging. All Products must be delivered in the manufacturer's standard package. Costs must include all packing and/or crating charges. Cases must be of durable construction, in good condition, properly labeled and suitable in every respect for storage and handling of contents. Each shipping carton must be marked with the commodity, brand, quantity, item code number and the Purchasing Entity's Purchase Order number.

IX. Inspection and Acceptance

IX.1 Laws and Regulations. Any and all Products offered and furnished must comply fully with all applicable Federal, State, and local laws and regulations.

IX.2 Applicability. Unless otherwise specified in the Master Agreement, Participating Addendum, or ordering document, the terms of this Section IX will apply. This section is not intended to limit rights and remedies under the applicable commercial code.

IX.3 Inspection. All Products are subject to inspection at reasonable times and places before acceptance. Contractor shall provide right of access to the Lead State, or to any other authorized agent or official of the Lead State or other Participating or Purchasing Entity, at reasonable times, to monitor and evaluate performance, compliance, and/or quality assurance requirements under this Master Agreement.

IX.3.1 Products that do not meet specifications may be rejected. Failure to reject upon receipt, however, does not relieve the Contractor of liability for material (nonconformity that substantially impairs value) latent or hidden defects subsequently revealed when goods are put to use.

IX.3.2 Acceptance of such goods may be revoked in accordance with the provisions of the applicable commercial code, and the Contractor is liable for any resulting expense incurred by the Purchasing Entity related to the preparation and shipping of Product rejected and returned, or for which acceptance is revoked.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

IX.4 **Failure to Conform.** If any services do not conform to contract requirements, the Purchasing Entity may require the Contractor to perform the services again in conformity with contract requirements, at no increase in Order amount. When defects cannot be corrected by re-performance, the Purchasing Entity may require the Contractor to take necessary action to ensure that future performance conforms to contract requirements and reduce the contract price to reflect the reduced value of services performed.

IX.5 **Acceptance Testing.** Purchasing Entity may establish a process, in keeping with industry standards, to ascertain whether the Product meets the standard of performance or specifications prior to acceptance by the Purchasing Entity.

IX.5.1 The acceptance testing period will be forty-five (45) calendar days, unless otherwise specified, starting from the day after the Product is delivered or, if installed by Contractor, the day after the Product is installed and Contractor certifies that the Product is ready for acceptance testing.

IX.5.2 If the Product does not meet the standard of performance or specifications during the initial period of acceptance testing, Purchasing Entity may, at its discretion, continue acceptance testing on a day-to-day basis until the standard of performance is met.

IX.5.3 Upon rejection, the Contractor will have fifteen (15) calendar days to cure. If after the cure period, the Product still has not met the standard of performance or specifications, the Purchasing Entity may, at its option: (a) declare Contractor to be in breach and terminate the Order; (b) demand replacement Product from Contractor at no additional cost to Purchasing Entity; or, (c) continue the cure period for an additional time period agreed upon by the Purchasing Entity and the Contractor.

IX.5.4 Contractor shall pay all costs related to the preparation and shipping of Product returned pursuant to the section.

IX.5.5 No Product will be deemed Accepted and no charges will be paid until the standard of performance or specification is met.

X. Warranty

X.1 **Applicability.** Unless otherwise specified in the Master Agreement, Participating Addendum, or ordering document, the terms of this Section X will apply.

X.2 **Warranty.** The Contractor warrants, for hardware Products (if applicable) for a period of one year from the date of acceptance, and for software Products and Services for a period of 90 days from the date of acceptance, that: (a) the Product performs according to all specific claims that the Contractor made in its response to the Solicitation, (b) the Product is suitable for the ordinary purposes for which such Product is used, (c) the Product is suitable for any special purposes identified in the Solicitation or for which the Purchasing Entity has relied on the Contractor's skill or judgment, (d) the Product is designed and manufactured in a commercially reasonable manner, and (e) the Product is free of defects.

X.3 **Breach of Warranty.** Upon breach of the warranty set forth above, the Contractor will repair or replace (at no charge to the Purchasing Entity) the Product whose nonconformance is discovered and made known to the Contractor. If the repaired and/or replaced Product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made.

X.4 **Rights Reserved.** The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation, actual damages, and, as applicable and awarded under

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

the law, to a prevailing party, reasonable attorneys' fees and costs.

X.5 Warranty Period Start Date. The warranty period will begin upon acceptance, as set forth in Section IX.

XI. Product Title

XI.1 Conveyance of Title. If both the Contractor and Purchasing Entity intend for any Products or Services being purchased to be owned by the Purchasing Entity after the sale (as opposed to a subscription service, service term, or other right of use), upon acceptance by the Purchasing Entity, Contractor shall convey to Purchasing Entity title to the Product free and clear of all liens, encumbrances, or other security interests.

XI.2 Embedded Software. Transfer of title to the Product must include an irrevocable and perpetual license to use any Embedded Software in the Product. If Purchasing Entity subsequently transfers title of the Product to another entity, Purchasing Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title. A subsequent transfer of this software license will be at no additional cost or charge to either Purchasing Entity or Purchasing Entity's transferee.

XI.3 License of Pre-Existing Intellectual Property. Contractor grants to the Purchasing Entity a nonexclusive, perpetual, royalty-free, irrevocable, license to use, publish, translate, reproduce, transfer with any sale of tangible media or Product, perform, display, and dispose of the Intellectual Property, and its derivatives, used or delivered under this Master Agreement, but not created under it ("Pre-existing Intellectual Property"). The Contractor shall be responsible for ensuring that this license is consistent with any third-party rights in the Pre-existing Intellectual Property.

XII. Indemnification

XII.1 General Indemnification. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers and employees, from and 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 arising from any act, error, or omission of the Contractor, its employees or Subcontractors or volunteers, at any tier, relating to performance under this Master Agreement.

XII.2 Intellectual Property Indemnification. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers and employees ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use infringes Intellectual Property rights of another person or entity ("Intellectual Property Claim").

XII.2.1 The Contractor's obligations under this section will not extend to any combination of the Product with any other product, system or method, unless the Product, system or method is:

XII.2.1.1 provided by the Contractor or the Contractor's subsidiaries or affiliates;

XII.2.1.2 specified by the Contractor to work with the Product;

XII.2.1.3 reasonably required to use the Product in its intended manner, and the infringement could not have been avoided

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

by substituting another reasonably available product, system or method capable of performing the same function; or

XII.2.1.4 reasonably expected to be used in combination with the Product.

XII.2.2 The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of the Intellectual Property Claim. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible.

XII.2.3 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 the Intellectual Property Claim 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.

XII.2.4 Unless otherwise set forth herein, Section 12.2 is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

XIII. Insurance

XIII.1 Term. Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. A Participating Entity may negotiate alternative Insurance requirements in their Participating Addendum.

XIII.2 Class. 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 A.M. Best's Insurance 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.

XIII.3 Coverage. Coverage must be written on an occurrence basis. The minimum acceptable limits will be as indicated below:

XIII.3.1 Contractor shall maintain Commercial General Liability insurance 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 and $2 million general aggregate;

XIII.3.2 CLOUD MINIMUM INSURANCE COVERAGE:

	Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions
Level of Risk	Minimum Insurance Coverage

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

XIII.3.3 Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

XIII.4 Notice of Cancellation. Contractor shall pay premiums on all insurance policies. Contractor shall provide notice to a Participating Entity who is a state within five (5) business days after Contractor is first aware of expiration, cancellation or nonrenewal of such policy or is first aware that cancellation is threatened or expiration, nonrenewal or expiration otherwise may occur.

XIII.5 Notice of Endorsement. 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) provides that written notice of cancellation will be delivered in accordance with the policy provisions, and (2) provides that the Contractor's liability insurance policy will be primary, with any liability insurance of any Participating State as secondary and noncontributory.

XIII.6 Participating Entities. Contractor shall provide to Participating States and Participating Entities the same insurance obligations and documentation as those specified in Section XIII, except the endorsement is provided to the applicable Participating State or Participating Entity.

XIII.7 Furnishing of Certificates. Contractor shall furnish to the Lead State copies of certificates of all required insurance in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement and prior to performing any work. Copies of renewal certificates of all required insurance will be furnished within thirty (30) days after any renewal date to the applicable state Participating Entity. The Lead State or a Participating Entity may request proof of insurance and copies of certificates of insurance at any time during the term of the Master Agreement. Failure to provide evidence of coverage may, at the sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

XIII.8 Disclaimer. Insurance coverage and limits will not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

XIV. General Provisions

XIV.1 Records Administration and Audit

XIV.1.1 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 will 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 will survive for a

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

period of six (6) years following termination of this Agreement or final payment for any Order placed by a Purchasing Entity against this Master Agreement, whichever is later, or such longer period as is required by the Purchasing Entity's State statutes, to assure compliance with the terms hereof or to evaluate performance hereunder.

XIV.1.2 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.

XIV.1.3 The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement that requires the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

XIV.2 Confidentiality, Non-Disclosure, and Injunctive Relief

XIV.2.1 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 or Purchasing Entity's clients.

XIV.2.1.1 Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity ("Confidential Information").

XIV.2.1.2 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.

XIV.2.1.3 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.

XIV.2.2 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

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Master Agreement.

XIV.2.2.1 Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information.

XIV.2.2.2 Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person.

XIV.2.2.3 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.

XIV.2.2.4 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.

XIV.2.3 **Injunctive Relief.** Contractor acknowledges that Contractor's breach of Section 14.2 would cause irreparable injury to the Purchasing Entity that cannot be adequately compensated in monetary 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.

XIV.2.4 **Purchasing Entity Law.** These provisions will be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

XIV.2.5 **NASPO ValuePoint.** The rights granted to Purchasing Entities and Contractor's obligations under this section will also extend to NASPO ValuePoint's Confidential Information, including but not limited to Participating Addenda, Orders or transaction Data relating to Orders under this Master Agreement that identify the entity/customer, Order dates, line-item descriptions and volumes, and prices/rates. This provision does not apply to disclosure to the Lead State, a Participating State, or any governmental entity exercising an audit, inspection, or examination pursuant to this Master Agreement. To the extent permitted by law,

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Contractor shall notify the Lead State of the identity of any entity seeking access to the Confidential Information described in this subsection.

XIV.2.6 Public Information. This Master Agreement and all related documents are subject to disclosure pursuant to the Lead State's public information laws.

XIV.2.7 Purchasing Entity Data. Purchasing Entity retains full rights and title to Data provided by it and any Data derived therefrom, including metadata. Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an Order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity. Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

XIV.2.7.1 Regarding Purchasing Entity Data related to an Artificial Intelligence (AI) solution purchased, the above section applies but may be negotiated on a state by state, case by case basis. Often AI models that are purchased to assist an entity, rely on having some type of access, license, and/or approval to use the data for the purpose of continually updating the AI model. This allows them to enhance, modify, and/or update the AI model so that the Purchasing Entity has the most up to date model for the best user experience. A Purchasing Entity has the default of section 14.2.7 applied unless a different standard is negotiated specific to AI.

XIV.3 Assignment/Subcontracts

XIV.3.1 Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

XIV.3.2 The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties, to NASPO ValuePoint and other third parties.

XIV.4 Changes in Contractor Representation. The Contractor must, within ten (10) calendar days, notify the Lead State in writing of any changes in the Contractor's key administrative personnel managing the Master Agreement. The Lead State reserves the right to approve or reject changes in key personnel, as identified in the Contractor's proposal. The Contractor shall 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.

XIV.5 Independent Contractor. Contractor is an independent Contractor. Contractor has 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 shall not to hold itself out as agent except as expressly set forth herein or as expressly set forth in an applicable Participating Addendum or Order.

XIV.6 Cancellation. Unless otherwise set forth herein, this Master Agreement may be canceled by either party upon sixty (60) days' written notice prior to the effective

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

date of the cancellation. Further, any Participating Entity may cancel its participation upon thirty (30) days' written notice, unless otherwise limited or stated in the Participating Addendum. Cancellation may be in whole or in part. Any cancellation under this provision will not affect the rights and obligations attending Orders outstanding at the time of cancellation, including any right of a Purchasing Entity to indemnification by the Contractor, rights of payment for Products delivered and accepted, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit. Cancellation of the Master Agreement due to Contractor default may be immediate.

XIV.7 Force Majeure. Neither party to this Master Agreement shall be held responsible for delay or default caused by one or more of the following events, if such occurrence or continuation of such occurrence is beyond the party's reasonable control and substantially inhibits the party's ability to deliver Product or other deliverables in accordance with this Master Agreement: fire, riot, unusually severe weather, other acts of God, acts of war or terrorism, and restrictions on the movement of people or goods imposed in a public health order or by a declared state of emergency. The Lead State may terminate this Master Agreement upon determining such delay or default will reasonably prevent successful performance of the Master Agreement

XIV.8 Defaults and Remedies

XIV.8.1 The occurrence of any of the following events will be an event of default under this Master Agreement:

XIV.8.1.1 Nonperformance of contractual requirements;

XIV.8.1.2 A material breach of any term or condition of this Master Agreement;

XIV.8.1.3 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;

XIV.8.1.4 Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

XIV.8.1.5 Any default specified in another section of this Master Agreement.

XIV.8.2 Upon the occurrence of an event of default, the Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of fifteen (15) calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure will not diminish or eliminate Contractor's liability for damages, including liquidated damages to the extent provided for under this Master Agreement.

XIV.8.3 If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Agreement and the Lead State shall have the right to exercise any or all of the following remedies:

XIV.8.3.1 Any remedy provided by law;

XIV.8.3.2 Termination of this Master Agreement and any related Contracts or portions thereof;

XIV.8.3.3 Assessment of liquidated damages as provided in this Master Agreement;

XIV.8.3.4 Suspension of Contractor from being able to respond to future bid solicitations;

XIV.8.3.5 Suspension of Contractor's performance; and

XIV.8.3.6 Withholding of payment until the default is remedied.

XIV.8.4 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 shall 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. Unless otherwise specified in an Order, a Purchasing Entity shall provide written notice of default as described in this section and have all of the rights and remedies under this paragraph and any applicable Participating Addendum with respect to an Order placed by the Purchasing Entity. Nothing in these Master Agreement Terms and Conditions will be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

XIV.9 Waiver of Breach. Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies will not operate as a waiver under this Master Agreement, any Participating Addendum, or any Purchase Order. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order will 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, any Participating Addendum, or any Purchase Order.

XIV.10 Debarment. The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in public procurement or contracting 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.

XIV.11 No Waiver of Sovereign Immunity

XIV.11.1 In no event will this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the 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

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

any claim or from the jurisdiction of any court.

XIV.11.2 This section applies to a claim brought against the Participating Entities who are states only to the extent Congress has appropriately abrogated the state's sovereign immunity and is not consent by the state to be sued in federal court. This section is also not a waiver by the 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.

XIV.12 Governing Law and Venue

XIV.12.1 The procurement, evaluation, and award of the Master Agreement will 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 will be governed by the law of the State serving as Lead State. The construction and effect of any Participating Addendum or Order against the Master Agreement will be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

XIV.12.2 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 state serving as Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement will 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 will be in the Purchasing Entity's state.

XIV.12.3 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; a Participating State if a named party; the state where the Participating Entity or Purchasing Entity is located if either is a named party.

XIV.13 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 in that state for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at the Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

XIV.14 Survivability. Unless otherwise explicitly set forth in a Participating Addendum or Order, the terms of this Master Agreement as they apply to the Contractor, Participating Entities, and Purchasing Entities, including but not limited to pricing and the reporting of sales and payment of administrative fees to NASPO ValuePoint, shall survive expiration of this Master Agreement and shall continue to apply to all Participating Addenda and Orders until the expiration thereof.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment A.1 – Software Publisher Terms and Conditions

The terms and conditions contained within Attachment A.1 cover the three following user options:

A. Software as a Service (SaaS)
B. Platform as a Service (PaaS)
C. Infrastructure as a Service (IaaS)

A. Software-as-a-Service (SaaS) Terms and Conditions

1. Definitions:

a. **Authorized Persons:** The service provider's employees, contractors, Subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. .

c. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

d. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

e. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notifications.

f. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

g. **Service provider:** The Contractor and its employees, Subcontractors, agents and affiliates who are providing the services agreed to under the contract. Service provider also includes a Third-party Provider providing services under the contract.

h. **Software-as-a-Service (SaaS):** The capability provided to the consumer to use the

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

provider's applications running on a 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.

i. **Statement of Work:** A Statement of Work (SOW) is a detailed document issued against the Master Agreement that defines the scope, deliverables, timelines, responsibilities, and acceptance criteria for Products and Services to be performed, ensuring clear expectations between the Contractor or Third-Party Provider and Purchasing Entities.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

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

a. The service provider 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 NIST SP 800- 53 (then current, or prior version compliant with the appropriate certification body's requirements) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

b. All data obtained by the service provider in the performance of this contract shall become and remain property of the public jurisdiction.

c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). Unless otherwise stipulated, the service provider is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the SLA, End User Agreement, or otherwise made a part of this contract.

d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

encryption for all non-public data shall be identified and made a part of this contract.

e. At no time shall any data or processes that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

f. The service provider shall not use any information collected in connection with the service issued from this contract for any purpose other than fulfilling the service.

4. Data Privacy: The service provider's privacy controls must also abide by the following:

a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) Privacy Controls.

b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) Privacy Controls.

5. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support (see also below regarding offshore access and follow the sun technical support).

6. Data Access: The service provider shall be responsible for:

a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800- 53 (then current, or prior version compliant with the appropriate certification body's requirements) Access Controls.

b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the Purchasing Entity for follow the sun technical support.

c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

7. Import and Export of Data: The public jurisdiction shall have the ability to import or export data:

a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract, End User Agreement, or SLA. This includes the ability for the public jurisdiction to import or export data to/from other service providers.

b. At intervals as frequent as the public jurisdiction requires.

8. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach.

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

b. **Security Incident Reporting Requirements:** The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in law, a Participating Addendum, or End User Agreement.

c. **Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within 48 hours or sooner — unless shorter time is required by applicable law — and take commercially reasonable measures to address the data breach in a timely manner.

9. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

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

b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures,

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.

10. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including Subcontractors, to fulfill obligations of the contract who have been convicted of any crime of dishonesty if such staff in fulfilling the obligations of the contract would have access to Purchasing Entity data or access onsite to Purchasing Entity's facilities. This includes but is not limited to criminal fraud or conviction of any felony or misdemeanor offense with an authorized penalty of up to one year of incarceration. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information. Each State/Participating Entity may have different background check requirements that must be followed for work performed in its jurisdiction, and such requirements would be discussed at the time a Participating Addendum is entered into.

11. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable NDAs and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

12. Right to Remove Individuals: The public jurisdiction may at any time require that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall notify the service provider of its determination and its reasons for requesting the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

13. Security: The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. The service provider's disclosures shall include information related to:

1. Governance and compliance
2. Standards and policies
3. Security and risk assessments
4. Continuous monitoring and alerting
5. Privilege and identity access management

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

6. Data protections
7. Infrastructure and application protections
8. Native cloud service provider security information and event management (SIEM)/log management tools
9. System health and resource monitoring
10. Incident response and recovery

The public jurisdiction and the service provider shall understand each other's roles and responsibilities for security and document them within the SLA or End User Agreement.

14. Access to Security Logs and Reports:

a. The service provider shall provide reports to the public jurisdiction in a format specified in the SLA or End User Agreement. Reports shall include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events (e.g., failed and successful events — system shutdown or starting a service, errors, anomalous/abnormal activity or system events, etc.), log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion, account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time) and transaction size (e.g., email message size, file transfer size, etc.), and security logs for all public jurisdiction data related to this contract.

b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers), virtualization/ hypervisor, operating system, middleware and runtime, applications and networking. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management; networking; and data. The methods and conditions for authorized access to logs/reports and the format for the logs/reports shall be specified and agreed upon by both parties in the SLA or End User Agreement. Specific shared responsibilities are identified in the SLA or End User Agreement.

15. Retention, Preservation and Archival of Security Logs and Reports: The service provider shall retain security logs and reports in a usable format for a minimum of 6 years and a maximum retention/archival of 6 years beyond the termination of the contract. The methods and timeframes for the retention, reservation (i.e., legal hold) and archival for the logs and reports will be specified and agreed upon by both parties in the SLA or End User Agreement.

16. Encryption of Data at Rest: The service provider shall prevent its employees and Subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.

17. Contract Audit: The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

18. Data Center Audit: An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with the provision of a cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable. Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with the provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.

19. Continuous Monitoring: The service provider shall, at service provider's expense, conduct continuous monitoring of its compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction:

a. Reliance on StateRAMP authorization and independent assessments by third-party assessment organizations (3PAOs)
b. Reliance on FedRAMP authorization and independent assessments by 3PAOs
c. Review of control documentation by internal staff or 3PAO
d. Acceptance of the service provider's third-party attestation (e.g. AICPA SOC2-Type 2 audit)
e. Self-assessment by service provider

20. Responsibilities and Uptime Guarantee: The service provider 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 responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA or End User Agreement.

21. Change Control and Advance Notice: The service provider shall give advance notice (to be determined at the contract time and included in the SLA or End User Agreement) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.

22. Subcontractor Disclosure: The service provider shall identify all of its strategic business partners related to services provided under this contract, 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 service provider, and who shall be involved in any application development and/or operations.

23. Business Continuity and Disaster Recovery:
The service provider shall provide a business continuity and disaster recovery plan upon request and ensure that the public jurisdiction's recovery time objective (RTO) is met.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

24. Compliance with Accessibility Standards:
The service provider shall comply with and adhere to accessibility standards of Section 508 Amendment to the Rehabilitation Act of 1973.

25. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

26. Subscription Terms: Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for SaaS, use underlying software as embodied or used in the service; and (3) view, copy, upload and download (where applicable), and use contractor's documentation.

27. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

28. Termination and Suspension of Service:

a. In the event of a contract termination, the service provider shall return public jurisdiction's data in a CSV or other mutually agreeable format at a time agreed to by the parties. The service provider also will provide for the subsequent secure disposal of public jurisdiction data.

b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction data.

c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of:

    1. 10 days after the effective date of termination, if the termination is in accordance with the contract period
    2. 30 days after the effective date of termination, if the termination is for convenience
    3. 60 days after the effective date of termination, if the termination is for cause

    After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d. The public jurisdiction 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 in the SOW.

e. The service provider shall securely dispose of all requested data in all forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

----------END of SaaS Terms and Conditions----------

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

B. Platform-as-a-Service (PaaS) Terms and Conditions

1. Definitions:

a. **Authorized Persons:** The service provider's employees, contractors, Subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

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

d. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

e. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

f. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

g. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

h. **Service Provider:** The Contractor and its employees, Subcontractors, agents and affiliates who are providing the services agreed to under the contract. Service provider also includes a Third-party Provider providing services under the contract.

i. **Statement of Work:** A Statement of Work (SOW) is a detailed document issued against the Master Agreement that defines the scope, deliverables, timelines, responsibilities,

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

and acceptance criteria for Products and Services to be performed, ensuring clear expectations between the Contractor or Third-Party Provider and Purchasing Entities.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at the public jurisdiction's written request.

3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions:

a. The service provider 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 within its control. Such security measures shall be in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction.

c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). The SLA or End User Agreement and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the Statement of Work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.

d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.

e. At no time shall any data or processes which either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

4. Data Privacy: The service provider's privacy controls must abide by the following:

a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) Privacy Controls.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) Privacy Controls.

5. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support (see also below regarding offshore access and follow the sun technical support).

6. Data Access: The service provider shall be responsible for:

a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800- 53 (then current, or prior version compliant with the appropriate certification body's requirements) Access Controls.

   Preventing any offshore access by service provider, employees and contractors, unless explicitly authorized by the Purchasing Entity for follow the sun technical support.

b. Maintaining government data and allowing downloading for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/ deletion to the public jurisdiction.

7. Import and Export of Data: The public jurisdiction shall have the ability to import or export data:

a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract, End User Agreement, or SLA. This includes the ability for the public jurisdiction to import or export data to/from other service providers.

b. At intervals as frequent as the public jurisdiction requires.

8. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach.

a. **Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

b. **Security Incident Reporting Requirements:** The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in law, a Participating Addendum, or End User Agreement.

c. **Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within 48 hours or sooner — unless shorter time is required by applicable law — and take commercially reasonable measures to address the data breach in a timely manner.

9. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider and related to the service provided under this contract.

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

   The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices.

b. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.

10. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including Subcontractors, to fulfill obligations of the contract who have been convicted of any crime of dishonesty if such staff in fulfilling the obligations of the contract

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

would have access to Purchasing Entity data or access onsite to Purchasing Entity's facilities. This includes but is not limited to criminal fraud or conviction of any felony or misdemeanor offense with an authorized penalty of up to one year of incarceration. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information. Each State/Participating Entity may have different background check requirements that must be followed for work performed in its jurisdiction, and such requirements would be discussed at the time a Participating Addendum is entered into.

11. Non-Disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.

12. Right to Remove Individuals: The public jurisdiction may at any time require the service provider to remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

13. Security: The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider.

1. The service provider's disclosures shall include information related to:
2. Governance and compliance
3. Standards and policies
4. Security and risk assessments
5. Continuous monitoring and alerting
6. Privilege and identity access management
7. Data protections
8. Infrastructure and application protections
9. Native cloud service provider SIEM/log management tools
10. System health and resource monitoring
11. Incident response and recovery

The public jurisdiction and the service provider shall understand each other's roles and responsibilities and document them within the SLA or End User Agreement.

14. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in a format as specified in the SLA or End User Agreement and agreed to by the service provider and the public jurisdiction. Reports will include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events (e.g., failed and successful events — system shutdown or starting a service, errors, anomalous/abnormal activity or system events, etc.), log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion,

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time) and transaction size (e.g., email message size, file transfer size, etc.), and security logs for all public jurisdiction data related to this contract.

a. The service provider and the public jurisdiction recognize that security responsibilities are shared. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers), virtualization/ hypervisor, operating system, middleware and runtime. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management; networking; and data. In certain instances, the public jurisdiction has sole responsibility for securing its applications and data that run within the PaaS computing environment. The methods and conditions for access to logs/reports and the format for logs/reports shall be specified and agreed upon by both parties in the SLA or End User Agreement. Specific shared responsibilities are identified in the SLA or End User Agreement.

15. Retention, Preservation and Archival of Security Logs and Reports: The service provider shall retain security logs and reports in a usable format for a minimum of 6 years and a maximum retention/archival of 6 years beyond the termination of the contract. The methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs and reports will be specified and agreed upon by both parties in the SLA or End User Agreement.

16. Encryption of Data at Rest: The service provider shall prevent its employees and Subcontractors from storing personal data on portable devices, except within data centers located in the United States. If personal data must be stored on portable devices to accomplish the work, the service provider must use hard drive encryption in accordance with cryptography standards referenced in FIPS 140-2, Security Requirements for Cryptographic Modules.

17. Contract Audit: The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of an NDA, to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

18. Data Center Audit: An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with the provision of a cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable.

Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with the provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.

19. Continuous Monitoring: The service provider shall, at service provider's expense, conduct continuous monitoring of its compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction:

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

a. Reliance on StateRAMP authorization and independent assessments by third-party assessment organizations (3PAOs)
b. Reliance on FedRAMP authorization and independent assessments by 3PAOs
c. Review of control documentation by internal staff or 3PAOs
d. Acceptance of the service provider's third-party attestation (e.g. AICPA SOC2-Type 2 audit)
e. Self-assessment by the service provider

20. Responsibilities and Uptime Guarantee: The service provider 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 environment are the responsibility of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime) and provide service to customers as defined in the SLA or End User Agreement.

21. Change Control and Advance Notice: The service provider shall give advance notice (to be determined at contract time and included in the SLA or End User Agreement) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.

22. Sub-Contractor Disclosure: The service provider shall identify all strategic business partners related to services provided under this contract, 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 service provider, and who will be involved in any application development and/or operations.

23. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure the public jurisdiction's recovery time objective (RTO) is met.

24. Compliance with Accessibility Standards: The service provider shall comply with and adhere to accessibility standards of Section 508 Amendment to the Rehabilitation Act of 1973.

25. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

26. Subscription Terms: Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for PaaS, use underlying software as embodied or used in the service; and (3) view, copy, upload and download (where applicable), and use the contractor's documentation.

27. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

28. Termination and Suspension of Service:

a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.

b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction digital content.

c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content.

d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/ DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

----------END of PaaS Terms and Conditions----------

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

C. Infrastructure-as-a-Service (IaaS) Terms and Conditions

1. Definitions:

a. **Authorized Persons:** The service provider's employees, contractors, Subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.

b. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

c. **d. Infrastructure-as-a-Service (IaaS):** 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, including 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). .

d. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

e. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

f. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

g. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non- public data within the possession or control of the service provider. A security incident may or may not turn into a data breach. .

h. **Service Provider:** The Contractor and its employees, Subcontractors, agents and affiliates who are providing the services agreed to under the contract. Service provider also includes a Third-party Provider providing services under the contract.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

i. **Statement of Work:** A Statement of Work (SOW) is a detailed document issued against the Master Agreement that defines the scope, deliverables, timelines, responsibilities, and acceptance criteria for Products and Services to be performed, ensuring clear expectations between the Contractor or Third-Party Provider and Purchasing Entities.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its public jurisdiction data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data except (1) during data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information within its control and comply with the following conditions:

a. The service provider 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 within its control. Such security measures shall be in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction.

c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). The SLA or End User Agreement and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.

d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. At no time shall any data or processes which either belong to or are intended for the use of public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

4. Data Privacy: The service provider's privacy controls must abide by the following:

a. No type of data mining may be performed on any public jurisdiction data without permission from the public jurisdiction. This includes mining location data from users of applications running on behalf of the public jurisdiction in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

requirements) Privacy Controls.

b. No public jurisdiction data may be sold or transferred to any third party, including service provider affiliates, without permission from the public jurisdiction in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) Privacy Controls.

5. Data Location: The service provider shall provide its services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support (see also below regarding offshore access and follow the sun technical support).

6. Data Access: The service provider is responsible for:

a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) Access Controls.

b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the Purchasing Entity for follow the sun.

c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

7. Import and Export of Data: The public jurisdiction shall have the ability to import or export data:

a. In piecemeal or in entirety at its discretion without interference and with support from the service provider as described in the contract, End User Agreement, or SLA. This includes the ability for the public jurisdiction to import or export data to/from other service providers.

b. At intervals as frequent as the public jurisdiction requires.

8. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any security incident or data breach.

a. **Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

b. **Security Incident Reporting Requirements:** The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in law, a Participating Addendum, or End User Agreement.

c. **Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within 48 hours or sooner — unless shorter time is required by applicable law and take commercially reasonable measures to address the data breach in a timely manner.

9. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of a service provider and related to service provided under this contract.

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

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

c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.

10. Background Checks: The service provider shall conduct criminal background checks and not utilize any staff, including Subcontractors, to fulfill obligations of the contract who have been convicted of any crime of dishonesty if such staff in fulfilling the obligations of the contract would have access to Purchasing Entity data or access onsite to Purchasing Entity's

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

facilities. This includes but is not limited to criminal fraud or conviction of any felony or misdemeanor offense with an authorized penalty of up to one year of incarceration. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information. Each State/Participating Entity may have different background check requirements that must be followed for work performed in its jurisdiction, and such requirements would be discussed at the time a Participating Addendum is entered into.

11. Non-Disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely necessary to perform job duties.

12. Right to Remove Individuals: The public jurisdiction may at any time require the service provider remove from interaction with the public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall notify the service provider of its determination and its reasons for requesting the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract or future work orders without the public jurisdiction's consent.

13. Security: The service provider shall disclose its non-proprietary security protocols, processes, tools and technical limitations to the public jurisdiction such that adequate protection and flexibility can be attained between the public jurisdiction and the service provider. The service provider's disclosures shall include information related to:

1. Governance and compliance
2. Standards and policies
3. Security and risk assessments
4. Continuous monitoring and alerting
5. Privilege and identity access management
6. Data protections
7. Infrastructure and application protections
8. Native cloud service provider SIEM/log management tools
9. System health and resource monitoring
10. Incident response and recovery

The public jurisdiction and the service provider shall understand each other's roles and responsibilities and document them within the SLA or End User Agreement.

14. Access to Security Logs and Reports:

a. The service provider shall provide reports to the public jurisdiction directly related to the infrastructure that the service provider controls upon which the public jurisdiction account resides. Unless otherwise agreed to in the SLA or End User Agreement, the service provider shall provide the public jurisdiction a history of all API calls for the public jurisdiction's account. This report shall include the identity of the API caller, the date and time of the API call, the source IP address of the API caller, the request

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

parameters, and the response elements returned by the service provider. The report will be sufficient to enable the public jurisdiction to perform security analysis, resource change tracking and compliance auditing.

b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers) and virtualization/hypervisor. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management; networking; and data. The public jurisdiction is responsible for its secure guest operating system, middleware, runtime, applications, firewalls and other logs captured within the guest operating system. The methods and conditions for access to logs/reports and the format for logs/reports are to be specified and agreed upon by both parties in the SLA or End User Agreement. Specific shared responsibilities are identified within the SLA or End User Agreement.

15. Retention, Preservation and Archival of Security Logs and Reports: The service provider shall retain security logs and reports in a usable format for a minimum of 6 years and a maximum retention/archival of 6 years beyond the termination of the contract. The methods and timeframes for the retention, preservation (i.e., legal hold), and archival for the logs and reports will be specified and agreed upon by both parties in the SLA or End User Agreement.

16. Encryption of Data at Rest: Not relevant to service model. Standards would be selected by the public jurisdiction.

17. Contract Audit: The service provider shall cooperate with public jurisdiction audit of conformance to the contract terms. The public jurisdiction or a contractor of its choice may perform the audit. The cost of the audit is the responsibility of the public jurisdiction. If information deemed confidential or proprietary must be reviewed during a contract compliance audit, either party may request the execution of a non-disclosure agreement (NDA), to the extent such agreements are allowed by the public jurisdiction's state law or municipal code.

18: Data Center Audit: An annual audit as required by StateRAMP and/or FedRAMP shall be performed for all relevant data centers associated with provision of the cloud service at the data center provider's expense. Providers must grant the government's information security office access to view the audit and artifacts through StateRAMP, if applicable.

a. Some governments may accept a SOC 2 Type 2 audit annually for all relevant data centers associated with provision of the cloud service at the service provider's expense. The audit must be made available to the jurisdiction if requested under unilateral NDA or after being redacted.

19. Continuous Monitoring: The service provider shall, at the service provider's expense, conduct continuous monitoring of its compliance with security controls required within the contract. Continuous monitoring shall be conducted via one or a combination of the following methods approved by the public jurisdiction:

a. Reliance on StateRAMP authorization and independent assessments by third-party assessment organizations (3PAOs)
b. Reliance on FedRAMP authorization and independent assessments by 3PAOs

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Review of control documentation by internal staff or 3PAOs

c. Acceptance of the service provider's third-party attestation (e.g. AICPA SOC2-Type 2 audit)
d. Self-assessment by the service provider

20. Responsibilities and Uptime Guarantee: The service provider 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 environment are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA or End User Agreement.

21. Change Control and Advance Notice: The service provider shall give advance written notice (to be determined at contract time and included in the SLA or End User Agreement) to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades or system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version to bring the system up to date or improve its characteristics. It usually includes a new version number.

22. Subcontractor Disclosure: The service provider shall identify all strategic business partners related to services provided under this contract, 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 service provider and who shall be involved in any application development and/or operations.

23. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan upon request and ensure the public jurisdiction's recovery time objective (RTO) is met.

24. Compliance with Accessibility Standards: Not relevant to service model. Standards would be selected by the public jurisdiction.

25. Web Services: Not relevant to service model. Standards would be selected by the public jurisdiction.

26. Subscription Terms: Contractor grants to a purchasing entity a license to: (1) access and use the service for its business purposes; (2) for IaaS, use underlying software as embodied or used in the service; (3) view, copy, upload and download (where applicable), and use contractor's documentation.

27. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

28. Termination and Suspension of Service:

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.

b. During any period of suspension, the service provider shall not intentionally erase any public jurisdiction digital content.

c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content.

d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/ DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

----------END of IaaS Terms and Conditions----------

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment A.2 – On-Premises Terms and Conditions

Due to the nature of on-premise software solutions, the Master Agreement defers these terms and conditions to be negotiated on a case by case basis by the entity seeking an on-premise software solution. As most Purchasing Entities will have very specific technology restrictions and/or statutes within its jurisdiction, creating a standard set of terms for this type of implementation was not reasonable. Each State and/or Participating Entity may add in specific on-premise terms and conditions to be negotiated at the time a Participating Entity seeks to enter a PA with an awarded Offeror.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment B
SCOPE OF WORK

This Scope of Work describes the solutions and services Contractor will provide through the Master Agreement.

The Master Agreement is not intended to replace or materially overlap in scope with other NASPO ValuePoint contract portfolios, including, but not limited to, the following:

1. Data Communications
2. eProcurement Solutions
3. Multi-Function Devices
4. Citizen Engagement Platforms
5. IT Research and Advisory Services
6. Audio Video Equipment, Software, and Services
7. MMIS
    a. Medicaid Enterprise Systems - Provider Services Module
    b. Medicaid Enterprise Systems - Claims Processing and Management Services Module
    c. Medicaid Enterprise Systems - Third Party Liability
    d. Medicaid Enterprise Systems - Pharmacy Benefits Manager (PBM)

Contractor may include equipment, accessories, and services available under these portfolios only to the extent that such solutions are complementary to the equipment, products, or services being offered. The Lead State may, at its sole discretion, reject products and services from a Contractor's catalog, or remove products and services from a Contractor's Master Agreement, if the Lead State determines that such products and services exceed the intended scope of this Master Agreement or do not comply with this requirement.

I. Scope of Work Overview:

This Scope of Work includes the award categories listed below. For any awarded category, Contractor may also provide related Value-Added Services. Contractor's awarded categories are listed below:

1. Direct Service Provider: SAAS
2. Direct Service Provider: Iaas
3. Direct Service Provider: On-Premise
4. Direct Service Provider: Value Added Services
5. Value-Added Reseller: SAAS
6. Value-Added Reseller: Iaas
7. Value-Added Reseller: On-Premise
8. Value-Added Reseller: Value Added Services

Hardware is generally not within the scope of this Master Agreement, however, some hardware that is an integral part of a Cloud or On-premises solution may be sold as part of an overall solution. Hardware is not available as a standalone purchase from the Master Agreement and Participating Addenda, except as replacement parts as needed for previously purchased hardware that was not purchased as a standalone but rather was incidental, ancillary, and/or required as part of an overall Cloud or On-Premises solution purchased under this contract. Internet Service Provider services are not within the scope of this Master Agreement.

Definitions:

Cloud and other software services terminology varies greatly within the information technology industry. To clarify the target audience and the intent of the Master Agreement, the following definitions shall apply:

1. Definitions, Roles, and Responsibilities:

Direct Service Providers: A Direct Service Provider is the entity responsible for making a service available to Purchasing Entities. A Direct Service Provider for a cloud solution or other software solution could include an original equipment manufacturer ("OEM"), software publisher, etc. A Direct Service

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Provider for purposes of the Master Agreement is an entity who creates and has its own solutions, and provides their own cloud or software solutions or services, and typically sets the pricing for its own Products and Services that it provides. A Direct Service Provider may or may not necessarily sell directly to customers and Purchasing Entities (it may onboard and utilize Fulfillment Partners and sell through the Fulfillment Partners exclusively as its authorized resellers as an example). A Direct Service Provider for an On-Premises solution would develop, maintain and support software that is installed locally on a consumer's system, hardware, or infrastructure and which is provided as Product under the Master Agreement.

A Direct Service Provider is responsible for all obligations and performance under its Master Agreement including all Products and Services, solutions, etc. provided by its Subcontractors, Fulfillment Partners, or Third-party Providers.

Value-added Reseller: A Value-added Reseller is an entity which primarily resells or distributes products, software, solutions, services, etc. that are developed and provided by a Subcontractor or Third-party Provider. Value-added Reseller may also include a firm, implementer, integrator, etc. that partners with a cloud or software solution provider, publisher, original equipment manufacturer ("OEM"), etc. to provide a solution. The value is generated by the Value-added Reseller's ability to help Purchasing Entities source multiple solutions through a one stop shop or to help create an overall cloud or software solution composed of multiple systems and services.

A Value-added Reseller is responsible for all obligations and performance under its Master Agreement, including all Products and Services, solutions, etc. provided by its Subcontractors, Fulfillment Partners, or Third-party Providers.

Fulfillment Partner: Is an agent authorized to act on behalf of a Contractor including a Contractor who is either a Direct Service Provider or Value-added Reseller. Fulfillment Partners may act as an authorized reseller, implementer, service provider, or other related role to fulfill and complete the delivery and performance of a Product or solution that is being purchased through a Master Agreement. Fulfillment Partners may quote, invoice, and receive payment on behalf of a Contractor. To add a Fulfillment Partner to a Master Agreement, the Contractor must submit a request to the Lead State for approval providing the Fulfillment Partner's vendor information, W-9, and updated list of Fulfillment Partners containing their contact information, which states/areas they are authorized to act in, and other pertinent information related to the products, services, solutions, etc. Fulfilment Partners are authorized to provide Products or resell on behalf of the Contractor.

A Contractor, whether in their role as a Direct Service Provider or Value-added Reseller (i.e. the Master Agreement holders), is fully responsible for all actions and performance of its Fulfillment Partners. A Purchasing Entity typically should not need to sign an End User Agreement to utilize a Fulfillment Partner because the Fulfillment Partner is acting on behalf of the primary Contractor and has been approved by the Lead State.

Subcontractor: A Subcontractor may be onboarded by a Contractor to provide additional Products and Services that are within the Contractor's Master Agreement award(s). A Subcontractor may include a software publisher, OEM, cloud provider, service provider, consultant, implementer, etc. and will provide Products and Services on a Contractor's Master Agreement in accordance with the terms and conditions of the Master Agreement. Because a Contractor is fully responsible for a Subcontractor and Subcontractor's Products and Services, the Subcontractor is not required to sign a Third-party Provider Agreement, but Contractor must have a Subcontractor approved by the Lead State to add its Products and Services to Contractor's Master Agreement (see Catalog Updates below). Contractor must ensure when onboarding a Subcontractor that the Subcontractor understands and accepts that the Master Agreement's and applicable Participating Addendum's terms and conditions will apply to Subcontractor's Products and Services when sold and provided through the Contractor's Master Agreement. Additionally, if a Subcontractor requires an End User Agreement, the Contractor must ensure its Subcontractors understand and accept the Order of Precedence outlined in the Master Agreement and where the Subcontractor's End User Agreements falls within the Order of Precedence. All End User Agreements for Subcontractors must meet the requirements outlined in the Master Agreement.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Subcontractors may not quote, invoice, or receive payment on behalf of a Contractor unless they are set up as a Fulfillment Partner by the Contractor and approved by the Lead State.

Third-party Provider: A Third-party Provider is not a Contractor and does not hold a Master Agreement. A Third-party Provider is a third-party publisher, developer, service provider, OEM, etc. who has executed a Third-party Provider Agreement with a Contractor and which has been approved by the Lead State. After executing a Third-party Provider agreement with a Contractor and receiving approval from the Lead State, a Third-party Provider allows their products, solutions, services, etc. to be sold and provided through the Contractor's Master Agreement. By executing a Third-party Provider Agreement with a Contractor and receiving approval from the Lead State, a Third-party Provider becomes party to the Master Agreement as a Third-party Provider as defined in the Master Agreement. In their role as a Third-party Provider, it agrees to, is bound by, and required to perform in accordance with all the terms and conditions of the Master Agreement and applicable Participating Addendum as it relates to all Products and Services it offers under the Master Agreement. This includes but is not limited to, that all its Products comply with all security standards/requirements, insurance requirements, and acknowledge the Order of Precedence contained in the Master Agreement.

Contractor, whether in a role as a Direct Service Provider or a Value-added Reseller, may utilize Third-party Providers in accordance with the terms of its Master Agreement. Because Third-party Providers receive compensation and a benefit for providing their Products and Services through a Master Agreement, and sign a Third-party Provider Agreement, it is the intent of the parties that both the Third-party Providers and Contractors are jointly and severally liable for the Products provided by a Third-party Provider. Third-party Providers are not responsible or liable for Products and Services provided by other Third-party Providers, only joint and severally liable, along with the Contractor, for the Products and Services the Third-party Provider itself offers. Contractor will always serve as the main points of contact for Purchasing Entities and Participating Entities for any and all issues related to the performance and delivery of Products provided under the Master Agreement. Contractors must make best efforts to assist Purchasing Entities and Participating Entities with any issues involving Third-party Providers that the Contractor may not have direct control over. A Third-party Provider is liable for the Products it provides via the Master Agreement in accordance with the Master Agreement, Participating Addendum, and applicable End User Agreement terms and conditions. Any breach of the Master Agreement, Participating Addendum, and applicable End User Agreement terms and conditions by the Third-party Provider may be enforced against the Third-party Provider as though it were a Contractor and signatory to the Master Agreement.

A template of the Third-party Provider Agreement to be executed at a later date between a Contractor and Third-party Provider is attached to the Master Agreement. Unless and until a Third-party Provider Agreement is executed between the Contractor and Third-party Provider, approved by the Lead State, and posted on NASPO ValuePoint's website on the Contractors landing page, it is not considered a valid agreement.

Third-party Providers may not quote, invoice, or receive payment on behalf of a Contractor unless they are set up as a Fulfillment Partner by the Contractor and approved by the Lead State.

Software Online Marketplace: A software online marketplace is a curated digital storefront or online catalog where customers can find, buy and manage software, data, services, etc. Use of a software online marketplace or digital catalog (e.g. AWS Marketplace, Azure Marketplace, etc.) by a Contractor is allowable to sell a Contractor's Products and Services (including Products and Services it may offer through Subcontractors or Third-party Providers), but only if there is a process through the online marketplace to incorporate the terms and conditions of the Contractor's Master Agreement and applicable Participating Addendum, and Contractor ensures the correct process for doing so is completed. Before any Subcontractor's, or Third-party Provider's solution may be sold by the Contractor via the online marketplace the Subcontractor or Third-party Provider Products and Services must be properly onboarded to Contractor's Master Agreement, including receiving approval from the Lead State (see above regarding Subcontractors and Third-party Providers, and see below regarding Catalog Updates).

2. Categorization of Risk

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Contractor must store and secure one, all, or a combination of data[1] Risk categories of the data are defined as:

a. Low Risk Data

Definition: FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Low Impact levels are defined in FIPS 199 as follows:

The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- Results in minor damage to organizational assets, minor financial loss, or minor harm to individuals.

b. Moderate Risk Data

Definition: FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- Result in significant damage to organizational assets, significant financial loss, or significant harm to individuals, but not loss of life or serious life-threatening injuries.

c. High Risk Data

Definition: FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("High Impact Data").

The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- Result in major damage to organizational assets, major financial loss, or severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Prior to signing a Participating Addendum, a Contractor and a Participating State must cooperate and determine what type of risk categories of the data are going to be utilized in the Participating Addendum.

[1] Data types and classifications may vary depending on the Participating State's laws and regulations. Participating States may change the classification levels, types, names, and restrictions for certain data during the participating addendum stage.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

3. Service Models

All Cloud Service Based Models must follow the NIST definition of cloud computing in NIST Special Publication 800-145. Any applicable standards for such Service Model identified in NIST 800-145 and 800-53 will apply to those Service Models that the Contractor was awarded. Additionally, all solutions and services (whether a Cloud Service Based Model or On-premise) must comply with NIST Special Publication 800-53 and any other applicable NIST standards.

Award Categories:

Below is not considered an exhaustive list of all the available types of cloud or software services that may be available. Often newer solution types may be a combination or a hybrid variation of the below categories. For example, Wi-Fi as a Service may be allowable as it's a combination of SaaS, IaaS and professional services.

All service models must align with all applicable NIST requirements and standards. The 4 main software services models and award categories are defined as:

1. **Software as a Service (SaaS) -** as used in this Master Agreement is defined as the capability provided to the consumer to use the provider's applications running on a 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. Full terms and conditions applicable to SaaS are located in Attachment A NASPO Master Agreement Terms and Conditions.

2. **Infrastructure as a Service (IaaS)** - as used in this Master Agreement is defined as the capability provided to the consumer for 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). Full terms and conditions applicable to IaaS are located in Attachment A NASPO Master Agreement Terms and Conditions.

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

4. **On-Premises** – as used in this Master Agreement is defined as Products and Services installed or provided locally on a consumer's hardware, servers, or other infrastructure. On-Premises solutions are not cloud solutions. Consumer maintains and has control over their operating systems, hardware, and infrastructure. Appropriate terms and conditions applicable to On-Premises solutions are being deferred to Participating Entities to negotiate in its Participating Addendum (PA). As On-Premises solutions are unique to each entity and involve individual jurisdictions and applicable code, rule, regulations, and statutes that will oversee this Service Model. This allows each Participating Entity to place its own mandatory requirements.

Value Added Services – Value Added Services includes a variety of professional services such as implementation, consulting, data migration, customization, configuration, installation, setup, etc. Value Added Services must fall within the general scope of an awarded category above.

4. Deployment Models

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Contractor must provide software services through one of the following deployment methods:

a. **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
b. **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
c. **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
d. **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)
e. **On-Premises.** software is installed and runs on computers on the premises of the person or organization using the software, rather than at a remote facility such as a server farm or cloud. In an On-Premises model the hardware and infrastructure is owned and maintained by the Purchasing Entity.

Note: In order to comply with NIST Standards and Requirements but encourage the development and use of new technologies and as new definitions or modifications of NIST Standards and Requirements are established, the scope of services for the Master Agreement may be modified to align with those definitions, pursuant to Utah Administrative Code R33-12-502. The scope of services may be modified for the Contract if both parties agree to the modification. Contract may not be extended beyond the terms of the contract included in this Master Agreement as a result of a modification.

II. NEW TECHNOLOGY

Pursuant to Utah Administrative Rule R33-12-502 the awarded contract(s) may be modified to incorporate new technology or technological upgrades associated with the procurement item being solicited, including new or upgraded: (i) systems; (ii) apparatuses; (iii) modules; (iv) components; and (v) other supplementary items. Further, a maintenance or service agreement associated with the procurement item under the resulting contract(s) may be modified to include any new technology or technological upgrades. Any contract modification incorporating new technology or technological upgrades will be specific to the procurement item being solicited and substantially within the scope of the original procurement or contract.

III. CATALOG UPDATES

Contractor may only add new Products and Services to their pricing catalog for those categories (i.e., service models - SaaS, IaaS, PaaS, and/or On-premises) that it was awarded.

At a minimum, Contractor's detailed catalog must identify the name and description of the Product offered, the Product provider's name, and the role of the Product provider under the Contract (e.g. Fulfilment Partner, Subcontractor, or Third-party Provider). Contractor catalog must list all Products and Services with SKUs (or some equivalent identifiers) and pricing. Pricing must demonstrate the correct contract price with the MSRP (or list price or equivalent if MSRP is not available), discount percentage, and Master Agreement price clearly listed. Additionally, Contractor must provide a summary catalog document listing all the solutions' names and Products available on the Master Agreement, but without all the pricing, line items, and SKU details. This will help Participating Entities more easily see what is available in a much more accessible document than the full detailed catalog.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Contractor is limited to one catalog and End User Agreement update **per quarter**. To add new Products and Services, the Contractor must submit the following information and documents to the State Lead for approval:

1. A brief description of the Product(s) to be added;
2. The category of the Product that falls within one of the Contractor's awarded categories (i.e. SaaS, PaaS, IaaS, On-Premises, Value Added Services);
3. An updated catalog/price list with a clear description of the Products offered and the category they fall under (SaaS, IaaS, PaaS, On-Premises, or Value Added Services);
4. Any additional terms and conditions that accompany the additional Products and Services, including End User Agreements that will be added to Master Agreement Attachment E. The Lead State will review these additional terms and conditions and End User Agreements to ensure their form complies with requirements in the Master Agreement. The Lead State approving of the addition of End User Agreements to the Master Agreement is not acceptance for purposes of making a purchase, and any additional terms and End User Agreements may be negotiated as needed by Participating Entities and individual Purchasing Entities at the time of ordering and making a purchase.
5. A certification that new catalog additions,(including any Products and Services offered via Subcontractors, Fulfillment Partners, and/or Third-party Providers) meet all the Terms & Conditions and requirements of the Master Agreement. An email message certification will suffice.
6. A certification that the new additions comply with the mandatory minimum discount % (and if applicable maximum mark up percentage for Value-added Resellers) as required in Contractor's Master Agreement. An email message certification will suffice.
7. A copy of the executed Third-party Provider Agreement (using the template provided in the Master Agreement) with a Third-party Provider whose Products the Contractor is reselling or utilizing in an overall solution through its Master Agreement (if applicable).
8. Copies of certificates of insurance that meet the correct coverage amounts for all Third-party Providers as required by the Master Agreement and appropriate for the Products and Services they offer through the Contractor's Master Agreement (if applicable).

Once the new catalog and any applicable End User Agreements are approved by the Lead State, the updated catalog and, if applicable, new End User Agreements will be published on the NASPO ValuePoint website via a Google Drive link or similar file sharing system maintained by the Lead State. Contractor catalogs and other product documents approved by the Lead State and published on or accessible through NASPO ValuePoint's website are incorporated by reference to the Master Agreement. An amendment to the Contractor's Master Agreement is not required for a catalog update that is approved by the Lead State and published on NASPO ValuePoint's website.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment C Pricing Discounts and Schedule

The discount and mark up percentages that shall apply to the Contractor's catalog are outlined below.
The Contractor's detailed and summary catalogs, as described in Attachment B: Scope of Work, will be available on the NASPO ValuePoint website. Attachment C of the Master Agreement incorporates by reference catalogs approved by the Lead State and posted on the Contractor's landing page on NASPO ValuePoint's website.

Minimum Discount % Off MSRP	Software (Saas)	Infrastructure (Iaas)	Platform (Paas)	On-Premises	Value Added Services*
Direct Service Providers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	1.50%	1.50%	NA	1.50%	1.50%
Value-Added Resellers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	1.50%	1.50%	NA	1.50%	1.50%
Maximum Markup %	**Software (Saas)**	**Infrastructure (Iaas)**	**Platform (Paas)**	**On-Premises**	**Value Added Services***
Value-Added Resellers: Maximum Markup %	22%	22%	NA	22%	22%

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment D

Contractor's Response to the Solicitation

Both the solicitation and the Contractor's response to the solicitation will both be available on the NASPO website for transparency, less any information marked as confidential by the Contractor at the time of submission.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment E

End User Agreements

This Attachment E incorporates by reference the End User Agreements approved by the Lead State and posted on NASPO ValuePoint's website.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment F: Third-party Provider Agreement (Template)

Pursuant to, and in accordance with, Attachment B of Master Agreement [*insert master agreement* number] signed between Contractor and the Lead State of Utah (the "Master Agreement"), [*insert third-party publisher/provider's information* here] the "Third-party Provider" hereby acknowledges that it has received and reviewed a complete copy of the Master Agreement and agrees that upon execution of this Third-party Provider Agreement, such Third-party Provider shall become a Third-party Provider under the Master Agreement once this Third-party Provider Agreement is signed by the Contractor and approved by the Lead State. Third-Party Provider shall be fully bound by, and subject to, all of the covenants, terms, and conditions of the Master Agreement as if it were a Contractor as they apply to its role as a Third-party Provider, as that term is defined and used in the Master Agreement.

Contractor and Third-party Provider are joint and severally liable for all Products and Services, as that term is defined in the Master Agreement, provided by the Third-party Provider under the Contractor's Master Agreement.

Third-party Provider acknowledges that any Third-party Terms and/or End User Agreements included by Third Party Provider will not supersede either the Master Agreement terms and conditions nor any Participating Entities terms and conditions contained within its Participating Addendum (PA). Third-Party Provider's additional terms (if any) will follow the order of precedence as established in the Master Agreement. Any breach of the Master Agreement Terms and Conditions by the Third Party may be enforced against the Third Party as though they were a signatory to the Master Agreement.

Contractor and Third-party Provider acknowledge this Third-party Provider Agreement is not effective until it is approved by the Lead State and posted on NASPO ValuePoint's Website on the Contractor's landing page. Third-party Provider may not begin providing services, access to a solution, delivering equipment, or provide any other Deliverables via Contractor's Master Agreement until the Lead State has provided written approval to the Contractor, and this Third-party Provider Agreement is posted on NASPO ValuePoint's website.

Contractor Name:	Third-party Provider Name:
_____ Signature and Date	_____ Signature and Date
_____ Signer Name and Title	_____ Signer Name and Title

Lead State Approval:

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

Attachment G
IRS Publication 1075 Exhibit 7

Exhibit 7 Safeguarding Contract Language

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

(1) All work will be performed under the supervision of the contractor.

(2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

obligated to the agency under this contract.

(12) For purposes of this contract, the term “contractor” includes any officer or employee of the contractor with access to or who uses FTI, and the term “subcontractor” includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency’s security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency’s security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency’s security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

Docusign Envelope ID: 60112789-ECD5-8D2E-8108-4930590D46EF

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.