Participating Addendum
Contract Number 26PSX0003AK

This Participating Addendum ("Participating Addendum" or "Contract") is made by and between the State of Connecticut acting by its Department of Administrative Services ("DAS" or "Participating Entity"), in accordance with sections 4a-2, 4d-2 and 4a-53 of the Connecticut General Statutes, and DLT Solutions, LLC ("Contractor").

The Contractor and DAS agree as follows:

1. DAS and the Contractor are bound by the terms of National Association of State Procurement Officials ("NASPO") master agreement number LS4992, attached as Exhibit 1, entered into between the Contractor and the State of Utah, effective September 16, 2026, (the "Master Agreement") for the purchase of cloud and software solutions, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), On-premises, and Value-Added Services, as a direct service provider or as a reseller of such services, except as modified in Attachment 1.

2. This Participating Addendum shall be in effect from the date that the Connecticut Attorney General's Office approves it, as evidenced by its signature below (the "Effective Date").

3. The Contractor and DAS are not bound to any modifications to the Master Agreement dated after the date of this Participating Addendum, except by mutual written agreement.

4. For purposes of this Participating Addendum, references to the Lead State in the Master Agreement intended to be obligations of the Participating Entity or obligations of the Contractor to the Participating Entity, shall be interpreted to mean DAS. To the extent references to the Lead State are obligations of the State of Utah, said references shall not be interpreted to mean DAS.

5. Order of Precedence:

   A. This Contract and the Master Agreement shall be read to be consistent and complementary. Any ambiguity, conflict or inconsistency between them shall be resolved by giving priority to this Contract.

   B. To the extent that any provisions in the Master Agreement and this Contract address the same or substantially the same subject matter, the provisions in this Contract shall prevail and replace, in their entirety, the provisions in the Master Agreement addressing the same or substantially the same subject matter. To the extent any provisions in the Master Agreement are titled the same or similarly titled as a provision in this Contract, the provisions in this Contract replace, in their entirety, the same or similarly titled provisions in the Master Agreement. By way of example but not limitation, if a Service Level Agreement is executed with or included in the SOW, such language shall prevail over any similar language in the Master Agreement.

   C. Unless specifically included in this Contract, all terms listed or referenced in any solicitation documents or in the Contractor's response to any solicitation documents are excluded.

   D. Subject to the terms in this Section 5, all other terms in the Master Agreement not specifically deleted or modified in Attachment 1 remain in full force and effect as to the Contractor, DAS and the Client Agency.

6. The Contractor shall comply with the Connecticut Standard Terms, attached as Exhibit 2. As used in this Participating Addendum, the capitalized word "Contract" is deemed to refer to this Participating Addendum and its exhibits.

7. The Contractor shall comply with the Minimum Service Level Requirements, attached as Exhibit 3, which sets forth minimum performance standards and related requirements applicable to all Services provided under this Contract.

8. To the extent that DAS or the Client Agency fails to meet its obligations under this Participating Addendum, the Contractor's exclusive remedies will be to seek redress in accordance with applicable Connecticut law, including the claims commissioner process set forth in Chapter 53 of the Connecticut General Statutes concerning claims against the State.

9. Nothing in the Master Agreement as modified by this Participating Addendum shall be construed as a modification, compromise or waiver by DAS or the State of any rights or defenses of any immunities provided by Federal law or the laws of the State of Connecticut to the State of Connecticut or any of its officers and employees, which they may have had, now have or will have with respect to all matters arising out of the Master Agreement as modified by this Participating Addendum. To the extent that this section conflicts with any other section in the Master Agreement or any other section of this Participating Addendum, this section shall govern.

10. Any Purchasing Entity or Client Agency may issue purchase orders against this Participating Addendum. "Purchasing Entity" or "Client Agency" means any department, commission, board, bureau, agency, institution, public authority, office, council, association, instrumentality or political subdivision of the State of Connecticut, non-profit organization organized in the State of Connecticut and any entity identified in Conn. Gen. Stat. Sec. 4a-54, as applicable, who is authorized and chooses to make purchases under, and pursuant to the terms and conditions of, this Participating Addendum.

11. Notice

    a. All notices, demands, requests, consents, approvals or other communications required or permitted to be given or which are given with respect to this Contract (for the purpose of this Section 11 collectively called "Notices") shall be deemed to have been effected at such time as the notice is placed in the U.S. mail, first class and postage pre-paid, return receipt requested or placed with a recognized, overnight express delivery service that provides for a return receipt. All such Notices shall be in writing and shall be addressed as follows:

       If to DAS:

       State of Connecticut Department of Administrative Services
       Procurement Division
       450 Columbus Boulevard, Suite 1202
       Hartford, CT 06103

       Attention: Alison LaFrance, Contract Specialist

       If to the Contractor:

       DLT Solutions, LLC
       2411 Dulles Corner Park
       Herndon, VA 20171

       Attention: Steve Wells

    b. Details regarding invoices and all technical or day-to-day administrative matters pertaining to this Contract shall be directed to:

       Client Agency: The individual specified in the applicable Purchase Order.

       Contractor: The individual designated by Contractor in writing to the Client Agency.

12. Orders

Any order placed by a Client Agency shall be deemed to be a sale under and governed by the prices and terms of Exhibit 1, Master Agreement and this Participating Addendum. Client Agencies shall include the references to “Master Agreement No. LS4992” and “DAS Contract No. 26PSX0003AK” in all Purchase Orders.

The parties are executing this Participating Addendum on the date below their respective signatures.

DLT Solutions, LLC

By: Steve Wells

Printed Name: Steve Wells
Title: Vice President, PMO & Operations
Date: 10/27/2026

STATE OF CONNECTICUT
Department of Administrative Services

By:

Printed Name: Mark D. Raymond
Title: Chief Information Officer
Date: 11/2/2026

APPROVED AS TO FORM

STATE OF CONNECTICUT
Office of the Attorney General

By: Jeffrey Zeman Digitally signed by Jeffrey Zeman
Date: 2026.11.02 11:43:02 -05'00'

Name: Jeffrey Zeman
Title: Assistant Attorney General
Date:

Attachment 1
Deletions and Modifications

1. The last sentence in Subsection III.1.6 of Section III (Order of Precedence) of Attachment A (NASPO ValuePoint Master Agreement Terms and Conditions) of the Master Agreement which reads as follows is deleted in its entirety: “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.”

2. Section 12.1(General Indemnification) of Section XII (Indemnification) of Attachment A (NASPO ValuePoint Master Agreement Terms and Conditions) of the Master Agreement is deleted in its entirety and replaced with the following: “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 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.”

3. Section 12.2.4 of Section XII (Indemnification) of Attachment A (NASPO ValuePoint Master Agreement Terms and Conditions) of the Master Agreement is deleted in its entirety and replaced with the following: “Unless otherwise set forth herein, Section 12 is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.”

4. The last sentence in Section I.2 (Categorization of Risk) of Attachment B (Scope of Work) of the Master Agreement which reads as follows is deleted in its entirety: “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” and replaced with: “The applicable data risk classification shall be determined by the Purchasing Entity in connection with the applicable SOW, or other purchasing document.”

Contract # LS4992

STATE OF UTAH COOPERATIVE CONTRACT

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

DLT Solutions LLC		
Name		
2411 Dulles Corner Park		
Address		
Herndon	VA	20171
City	State	Zip

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

Contact Person Adam Pritchard Phone # 703-773-8988 Email adam.pritchard@dlt.com
Vendor #94622A 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

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

DocuSigned by:
Steve Wells
B9F4D1F3DE064E6...
Contractor's Signature

Steve Wells — Print Name
Vice President, Operations — Title
12/2/2025 — Date

STATE

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

12/3/2025
Date

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,

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

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

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

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

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

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

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

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.

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

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.

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.

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.

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.

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.

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

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

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

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

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

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,

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

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

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

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.

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

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

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

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,

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

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

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.

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

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----------

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,

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.

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

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

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,

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:

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

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----------

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.

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

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

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

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

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

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:

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----------

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.

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: Paas
4. Direct Service Provider: On-Premise
5. Direct Service Provider: Value Added Services
6. Value-Added Reseller: SAAS
7. Value-Added Reseller: Iaas
8. Value-Added Reseller: Paas
9. Value-Added Reseller: On-Premise
10. 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 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.

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

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.

[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.

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.

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

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.

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.

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)	2%	2%	2%	2%	2%
Value-Added Resellers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	2%	2%	2%	2%	2%
Maximum Markup %	Software (Saas)	Infrastructure (Iaas)	Platform (Paas)	On-Premises	Value Added Services*
Value-Added Resellers: Maximum Markup %	95%	95%	95%	95%	95%

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.

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.

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:

Exhibit 2 – Contract Number 26PSX0003AK
Connecticut Standard Terms

1. Definitions

a. Acceptance

Determination made by the Client Agency upon successful User Acceptance Test that the Deliverable has satisfied the Acceptance Criteria itemized in the SOW, performs to the Specifications, and fulfills the business and technical requirements of this Contract.

b. Acceptance Criteria

Client Agency requirements for Deliverable Acceptance.

c. Acceptance Date

The date the Client Agency accepts a Deliverable or System in accordance with this Contract.

d. Artificial Intelligence

Artificial Intelligence" has the same meaning as provided in Conn. Gen. Stat. § 4a-2e, as may be amended.

e. Business Day

A day of the week recognized by the Client Agency as a workday, exclusive of Saturdays, Sundays and any State or federal holiday.

f. Claims

All actions, suits, claims, demands, investigations, and proceedings of any kind, open, pending, or threatened, whether mature, un-matured, contingent, known or unknown, at law or in equity in any forum.

g. Client Agency Data

Any data or information of the Client Agency that Contractor receives or creates by any means and in any form in connection with this Contract, Deliverables or Performance, including data and information with respect to any one or more of the following: databases, systems, operations, facilities, and regulatory compliance.

h. Confidential Information

Any name, number or other information that may be used, alone or in conjunction with any other information, to identify a specific individual including, but not limited to, such individual's name, date of birth, mother's maiden name, motor vehicle operator's license number and residential address, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation. Without limiting the foregoing, Confidential Information shall also include any information that DAS classifies as "confidential" or "restricted." Confidential Information shall not include information that may be lawfully obtained from publicly available sources or from federal, state, or local government records which are lawfully made available to the general public.

i. Confidential Information Breach

Generally, an instance where an unauthorized person or entity accesses Confidential Information in any manner, including but not limited to the following occurrences: (1) any Confidential Information that is not encrypted or protected is misplaced, lost, stolen or in any way compromised; (2) one or more third parties have had access to or taken control or possession of any Confidential Information that is not encrypted or protected without prior written authorization from the State; (3) the unauthorized acquisition of encrypted or protected Confidential Information together with the confidential process or key that is capable of compromising the integrity of the

Confidential Information; or (4) if there is a substantial risk of identity theft or fraud to the Client Agency, the Contractor, or State.

j. Contractor IP

Contractor's materials, including proprietary algorithms, code or data and other intellectual property (1) in existence prior to this Contract, (2) created, developed or acquired during the Term but not exclusively for the State, or (3) identified as Contractor IP in the applicable SOW; or (4) otherwise developed or acquired independent of this Contract and employed by the Contractor in connection with the Deliverables.

k. Contractor Parties

Contractor's members, principals, directors, officers, shareholders, partners, managers, representatives, agents, servants, consultants, employees, Subcontractors, Fulfillment Partners, and Third-party Providers or any one of them or any other person or entity with whom the Contractor is in privity or with whom Contractor contracts to Perform under this Contract in any capacity.

l. Deliverable

Each (1) Good, Service, Maintenance Services, Improvement, Materials, Documentation, System, process or information of any type, whether stand-alone or intended as part of the integration of the System with existing hardware or software of the State, and whether or not used for administrative, maintenance, consulting, training, data warehousing, operations, support, hosting, or fulfillment of Performance; and (2) warranty of a Deliverable(s) that is listed in the Pricing Schedule or provided by Contractor as an element of Contractor's overall approach and solution to the requirements of this Contract. Any one of them or a combination of any of them may be developed or produced by Contractor or by a third party as a supplier or subcontractor to Contractor.

m. Documentation

All Specifications; all technical, systems and user reference manuals; all System documentation related to each component of the System, Deliverables and processes; and any Improvements to any of them.

n. Environmentally Preferable

"Environmentally Preferable" has the same meaning as provided in Conn. Gen. Stat. § 4a-67h, as it may be amended.

o. Goods

All things which are movable, including, but not limited to, supplies, materials, equipment, hardware, software, specially manufactured things, a component incorporated into another thing and things that are attached to real property and that may be severed from the real property without material harm to the things.

p. Improvement

Any Contractor changes, patches, corrections, repairs, replacements, additions, modifications, enhancements, updates, releases, revisions, error fixes, bug fixes or any new versions of Deliverables, or any combination of the foregoing, that are to be or may be provided as a Deliverable from time to time. An Improvement may serve any purpose. Improvements do not include upgrades to software for which Contractor charges its customers, or upgrades by a Licensor that is charging Contractor for such upgrade.

q. Maintenance Services

The software and process support services described in this Contract, or a Statement of Work, as applicable.

r. Materials

Collectively, software programs, literary works, other works of authorship, documented

specifications, designs, analyses, processes, methodologies, concepts, inventions, know-how, programs, program listings, program tools, Documentation, reports, drawings, data bases, spreadsheets, machine readable text, models and work product, whether tangible or intangible.

s. Perform

All acts and things of the Contractor and Contractor Parties, severally and collectively, that are necessary or appropriate to fulfill or accomplish this Contract fully, including the Deliverables and all other Contract obligations. The word “Perform” includes all parts of speech.

t. Purchase Order

A written or electronic document that the Client Agency issues for one or more Deliverables in accordance with the terms of this Contract.

u. Records

All working papers and such other information and materials furnished or prepared by the Contractor in Performing including but not limited to, documents, data, plans, books, computations, drawings, specifications, notes, reports, records, estimates, summaries, memoranda and correspondence, kept or stored in any form.

v. Services

The labor or work, necessary or appropriate for the Contractor to Perform.

w. Site

Location(s) specified by the Client Agency where Deliverables are to be installed, Services rendered, or materials furnished.

x. Specifications

Contractor’s published technical and non-technical detailed descriptions of each Deliverable’s capabilities, or intended use or both, as more fully set forth in this Contract or a Statement of Work, as applicable.

y. State

The State of Connecticut, including DAS, the Client Agency and any office, department, board, council, commission, institution or other agency of the State.

z. Statement of Work (“SOW”)

Statement issued in connection with a Purchase Order for a Deliverable available under this Contract which sets forth all work and payment requirements for Contractor's Performance in connection with said Purchase Order, and may include a Service Level Agreement, if applicable

aa. System

Contractor furnished or otherwise supplied Deliverables that collectively and in an integrated fashion fulfill the Performance Criteria and the business and technical requirements of this Contract or SOW, as applicable.

bb. Term

The original term of this Contract plus any extensions exercised under this Contract.

cc. Termination

An end to this Contract prior to the end of its Term.

dd. Title

All ownership, title, licenses, rights and interest, including, but not limited to, perpetual use, of and to the Deliverable.

ee. User Acceptance Test

Those procedures that permit the State to authenticate and test the functionality of a Deliverable

with real world scenarios to determine if the Deliverable performs in accordance with this Contract.

2. Whistleblower Provision

This Contract may be subject to the provisions of section 4-61dd of the Connecticut General Statutes. In accordance with this statute, if an officer, employee or appointing authority of the Contractor takes or threatens to take any personnel action against any employee of the Contractor in retaliation for such employee's disclosure of information to any employee of the contracting state or quasi-public agency or the Auditors of Public Accounts or the Attorney General under the provisions of such statute, Contractor shall be liable for a civil penalty of not more than five thousand dollars for each offense, up to a maximum of twenty percent of the value of this Contract. Each violation shall be a separate and distinct offense and in the case of a continuing violation, each calendar day's continuance of the violation shall be deemed to be a separate and distinct offense. The State may request that the Attorney General bring a civil action in the Superior Court for the Judicial District of Hartford to seek imposition and recovery of such civil penalty. In accordance with such statute, each large state contractor, as defined in the statute, shall post a notice of the provisions of the statute relating to large state contractors in a conspicuous place which is readily available for viewing by the employees of the Contractor.

3. Disclosure of Records Concerning Governmental Functions

This Contract may be subject to the provisions of section 1-218 of the Connecticut General Statutes. In accordance with this statute, each contract in excess of two million five hundred thousand dollars between a public agency and a person for the performance of a governmental function shall (a) provide that the public agency is entitled to receive a copy of records and files related to the performance of the governmental function, and (b) indicate that such records and files are subject to FOIA and may be disclosed by the public agency pursuant to FOIA. No request to inspect or copy such records or files shall be valid unless the request is made to the public agency in accordance with FOIA. Any complaint by a person who is denied the right to inspect or copy such records or files shall be brought to the Freedom of Information Commission in accordance with the provisions of sections 1-205 and 1-206 of the Connecticut General Statutes.

4. Data: Access and Ownership

a. Access to Contract and State Data

The Contractor shall provide to the Client Agency access to any data, as defined in Conn. Gen Stat. Sec. 4e-1, concerning this Contract and the Client Agency that are in the possession or control of the Contractor upon demand and shall provide the data to the Client Agency in a format prescribed by the Client Agency and the State Auditors of Public Accounts at no additional cost.

b. Ownership of Data

1. All ownership, title, licenses, proprietary rights and interest (including, but not limited to, perpetual use) (for purposes of this Ownership of Data Section, collectively, “Title”) of and to any and all data as defined in section 4e-1 of the Connecticut General Statutes, ("Data") that is uploaded, collected, stored, held, hosted, located or utilized by the Client Agency or Contractor and Contractor Parties directly or indirectly in connection with this Contract at all times is and will always remain vested in the State. For the avoidance of doubt, Data shall include synthetic data and AI-generated content. At no time will Contractor have Title to such Data, wherever located.

2. At no cost to the State the Contractor and Contractor Parties shall, no later than fifteen (15) days after (i) receiving a written request from the Client Agency or (ii) Termination for any reason, deliver and transfer possession to the Client Agency all of the Data, in a format acceptable to the State.

3. At no cost to the State, the Contractor and Contractor Parties shall, no later than fifteen (15)

days, unless otherwise mutually agreed to in writing by the Parties, after (i) receiving a written request from the Client Agency, (ii) receiving final payment from the Client Agency, or (iii) Termination

4. for any reason, over-write and securely delete all of the Data, such that the Data will be expunged in a manner to make retrieval of the Data impossible.

The Contractor's failure to deliver and transfer possession of the Data to a duly authorized agent of the Client Agency shall constitute, without more, a de facto breach of this Contract. Consequently, the Contractor shall indemnify and hold harmless the Client Agency and the State, as appropriate, for any and all damages, costs and expenses associated directly or indirectly with such failure. The damages, costs and expenses shall include, but not be limited to, those resulting from any corresponding contracting for credit or identity protection services, or both, and from any subsequent non-State use of any Data. If Contractor Parties will Perform for any purpose under this paragraph, the Contractor represents and warrants that it shall cause each of the Contractor Parties to so Perform and that each has vested in the Contractor plenary authority to cause the Contractor Parties to Perform. For purposes of this Ownership of Data Section, "Perform" shall include, but not be limited to, the obligations relating to the sale, transfer of Title, removal and transfer of possession of the Data and indemnifying and holding harmless the Client Agency and the State. The Contractor on its own behalf and on behalf of the Contractor Parties shall also provide, no later than 30 days after receiving a request by the Client Agency, such information as the Client Agency may identify to ensure, in the Client Agency's sole discretion, compliance with the provisions of this Ownership of Data Section. This Ownership of Data Section survives Termination.

5. Forum and Choice of Law

The parties deem this Contract to have been made in the City of Hartford, State of Connecticut. Both parties agree that it is fair and reasonable for the validity and construction of this Contract to be, and it shall be, governed by the laws and court decisions of the State of Connecticut, without giving effect to its principles of conflicts of laws. To the extent that any immunities provided by Federal law or the laws of the State of Connecticut do not bar an action against the State, and to the extent that these courts are courts of competent jurisdiction, for the purpose of venue, the complaint shall be made returnable to the Judicial District of Hartford only or shall be brought in the United States District Court for the District of Connecticut only, and shall not be transferred to any other court, provided, however, that nothing here constitutes a waiver or compromise of the sovereign immunity of the State of Connecticut. The Contractor waives any objection which it may now have or will have to the laying of venue of any Claims in any forum and further irrevocably submits to such jurisdiction in any suit, action or proceeding.

6. State Comptroller's Specifications

In accordance with Conn. Gen. Stat. § 4d-31, this Contract is deemed to have incorporated within it, and Contractor shall deliver the Deliverables in compliance with, all specifications established by the State Comptroller to ensure that all policies, procedures, processes and control systems, including hardware, software and protocols, which are established or provided by Contractor or Contractor Parties, are compatible with and support the State's core financial systems, including but not limited to, accounting, payroll, time and attendance, and retirement systems.

7. Chief Information Officer Approval of Subcontractors

In accordance with Conn. Gen. Stat. § 4d-32, Contractor shall not award a subcontract for work under this Contract without having first obtained the written approval of the Chief Information Officer of the Department of Administrative Services or their designee of the selection of the subcontractor and of the provisions of the subcontract.

8. Ownership Rights and Integrity of Public Records

In accordance with Conn. Gen. Stat. § 4d-34, (a) neither Contractor nor Contractor Parties shall have any Title in or to (1) any public records which the Contractor or Contractor Parties possess, modify or

create pursuant to a contract, subcontract or amendment to a contract or subcontract, or (2) any modifications by such contractor, subcontractor, employee or agent to such public records; (b) neither Contractor nor Contractor Parties shall impair the integrity of any public records which they possess or create; and (c) public records which Contractor or Contractor Parties possess, modify or create pursuant to this Contract or other contract, subcontract or amendment to a contract or subcontract shall at all times and for all purposes remain the property of the State. For purposes of this Section, "public records" shall have the meaning set forth in Conn. Gen. Stat. § 4d-33, as it may be modified from time to time.

9. Application of FOIA to Public Records Provided to Contractor

In accordance with Conn. Gen. Stat. § 4d-35, any public record which a state agency provides to Contractor or Contractor Parties shall remain a public record for the purposes of subsection (a) of Conn. Gen. Stat. § 1-210 and as to such public records, the State, Contractor and Contractor Parties shall have a joint and several obligation to comply with the obligations of the state agency under the Freedom of Information Act (FOIA), as defined in Conn. Gen. Stat. §1-200, provided that the determination of whether or not to disclose a particular record or type of record shall be made by such state agency.

10. Nondisclosure of Public Records

In accordance with Conn. Gen. Stat. § 4d-36, neither Contractor nor Contractor Parties shall disclose to the public any public records (a) which they possess, modify or create pursuant to this Contract or any contract, subcontract or amendment to a contract or subcontract and (b) that a state agency (1) is prohibited from disclosing pursuant to state or federal law in all cases, (2) may disclose pursuant to state or federal law only to certain entities or individuals or under certain conditions or (3) may withhold from disclosure pursuant to state or federal law. This provision shall not be construed to prohibit the Contractor from disclosing such public records to any Contractor Parties to carry out the purposes of its subcontract. For purposes of this Section, "public records" shall have the meaning set forth in Conn. Gen. Stat. § 1-200, as it may be modified from time to time.

11. Profiting from Public Records

In accordance with Conn. Gen. Stat. § 4d-37, neither Contractor nor Contractor Parties shall sell, market or otherwise profit from the disclosure or use of any public records which are in their possession pursuant to this Contract or any contract, subcontract or amendment to a contract or subcontract, except as authorized in this Contract. For purposes of this Section, "public records" shall have the meaning set forth in Conn. Gen. Stat. § 1-200, as it may be modified from time to time.

12. Contractor's Obligation to Notify DAS Concerning Public Records

In accordance with Conn. Gen. Stat. § 4d-38, if the Contractor or Contractor Parties learn of any violation of the provisions of Conn. Gen. Stat. §§ 4d-36 or 4d-37 they shall, no later than seven calendar days after learning of such violation, notify the Chief Information Officer of such violation.

13. General Assembly Access to Records

In accordance with Conn. Gen. Stat. § 4d-40, the Joint Committee on Legislative Management and each nonpartisan office of the General Assembly shall continue to have access to DAS records that is not less than the access that said committee and such offices have on July 1, 1997.

14. Continuity of Systems

a. This Section is intended to comply with Conn. Gen. Stat. §4d-44. Nothing in this Section shall be construed to prevent Contractor from being paid for its Performance that is provided in accordance with this Contract.

b. Contractor acknowledges that the Deliverables, the Systems and associated Services are important to the function of State government and that they must continue without interruption. Pursuant to Conn. Gen. Stat. §4d-44, if the work under this Contract, any subcontract, or

amendment to either, is transferred back to the State or to another contractor at any time for any reason, then Contractor shall cooperate fully with the State, and do and Perform all acts and things that DAS deems to be necessary or appropriate, to ensure continuity of the Client Agency information system and telecommunication system facilities, equipment and Services so that there is no disruption or interruption in Performance as required or permitted in this Contract. Contractor shall not enter into any subcontract for any part of the Performance under this Contract without approval of such subcontract by DAS, as required by Conn. Gen. Stat. §4d-32 and without such subcontract including a provision that obligates the subcontractor to comply fully with Conn. Gen. Stat. §4d-44 as if the subcontractor were in fact the Contractor. Contractor shall make a full and complete disclosure of and delivery to DAS or its representatives of all Records and "Public Records," as that term is defined in Conn. Gen. Stat. §4d-33 in whatever form they exist or are stored and maintained and wherever located, directly or indirectly concerning this Contract.

c. The parties shall follow the below applicable and respective procedures in order to ensure the orderly transfer to the State:

   1. Facilities and Equipment:

      Unless a shorter period is necessary or appropriate to ensure compliance with Conn. Gen. Stat. §4d-44 , in which case that shorter period shall apply, Contractor shall deliver to the State, F.O.B. Hartford, Connecticut or other State location which the State identifies, all Deliverables, Systems, facilities and equipment related to or arising out of this Contract, subcontract or amendment, (other than any of the Deliverables, Systems, facilities or equipment in which Contractor has title under this Contract) no later than ten (10) days from the date that the work under this Contract is transferred back to the Client Agency or to another contractor for any reason. Contractor shall deliver the Deliverables, Systems, facilities or equipment to the State, during the State's business hours, in good working order and in appropriately protective packaging to ensure delivery without damage. Concurrent with this delivery, Contractor shall also deliver all related operation manuals and other Documentation in whatever form they exist and a list of all related passwords and security codes;

   2. Software Deliverables created or modified pursuant to this Contract, subcontract or amendment: Unless a shorter period is necessary or appropriate to ensure compliance with Conn. Gen. Stat. §4d-44, in which case that shorter period shall apply, Contractor shall deliver to the State, F.O.B. Hartford, Connecticut or other location which the Client Agency identifies, all Deliverables, Materials and Systems, no later than 10 days from the date that the work under the SOW or this Contract is transferred back to the State or to another contractor for any reason. Contractor shall deliver such Deliverables, Materials and Systems to the Client Agency, during the Client Agency's Business Hours, in good working order, and if the Client Agency's equipment shall be delivered, in appropriately protective packaging to ensure delivery without damage. Concurrent with this delivery, Contractor shall also deliver all Deliverable-related operation manuals and other Documentation in whatever form they exist, if delivery of such manuals and documentation is required by this Contract or the SOW for such Deliverable, and a list of all Deliverable passwords and security codes; and

   3. Public Records, as defined in Conn. Gen. Stat. §4d-33, which Contractor or Contractor Parties possess or create pursuant to this Contract, subcontract or amendment: Unless a shorter period is necessary or appropriate to ensure compliance with Conn. Gen. Stat. §4d-44, in which case that shorter period shall apply, Contractor shall deliver to the Client Agency, F.O.B. Hartford, Connecticut or other State location which Client Agency identifies, all Public Records created or modified pursuant to this Contract, any SOW, subcontract or amendment and requested in writing by the Client Agency (provided that Contractor may redact confidential information of Contractor, its personnel or third parties to the extent permitted by applicable law) no later than the latter of (1) the time specified in the section in this Contract concerning Termination for the return of Public Records and (2) ten (10) days from the date that the work under this Contract or SOW is transferred back to the Client Agency or to

another contractor for any reason. Contractor shall deliver to the Client Agency during the Client Agency's Business Hours those Public Records in electronic, magnetic or other intangible form in a non-proprietary format, such as, but not limited to, ASCII or TXT. Contractor shall deliver to the Client Agency, during the Client Agency's business hours, those Public Records and a list of all applicable passwords and security codes, all in appropriately protective packaging to ensure delivery without damage.

d. If Contractor employs former State employees, Contractor shall facilitate the exercising of any reemployment rights that such State employees may have with the State, including, but not limited to, affording them all reasonable opportunities during the workday to interview for State jobs. Contractor shall include language similar to this Section in all of its contracts with its subcontractors and applicable Contractor Parties so that they are similarly obligated.

15. Summary of State Ethics Laws

Pursuant to the requirements of section 1-101qq of the Connecticut General Statutes (a) the State has provided to the Contractor the summary of State ethics laws developed by the Office of State Ethics pursuant to section 1-81b of the Connecticut General Statutes, which summary is incorporated by reference into and made a part of this Contract as if the summary had been fully set forth in this Contract; (b) the Contractor represents that the chief executive officer or authorized signatory of the Contract and all key employees of such officer or signatory have read and understood the summary and agree to comply with the provisions of state ethics law; (c) prior to entering into a contract with any subcontractors or consultants, the Contractor shall provide the summary to all subcontractors and consultants and each such contract entered into with a subcontractor or consultant on or after July 1, 2021, shall include a representation that each subcontractor or consultant and the key employees of such subcontractor or consultant have read and understood the summary and agree to comply with the provisions of state ethics law; (d) failure to include such representations in such contracts with subcontractors or consultants shall be cause for Termination of the Contract; and (e) each contract with such contractor, subcontractor or consultant shall incorporate such summary by reference as a part of the contract terms.

16. Audit and Inspection of Plants, Places of Business and Records

a. The State and its agents, including, but not limited to, the Connecticut Auditors of Public Accounts, Attorney General and State's Attorney and their respective agents, may, at reasonable hours, inspect and examine all of the parts of the Contractor's and Contractor Parties' plants and places of business which, in any way, are related to, or involved in, the Performance of this Contract.

b. Contractor shall maintain, and shall require each Contractor Party to maintain, accurate and complete Records. Contractor shall make all of its and the Contractor Parties' Records available at all reasonable hours for audit and inspection by the State and its agents.

c. The State shall make all requests for any audit or inspection in writing and shall provide the Contractor with at least twenty- four (24) hours' notice prior to the requested audit and inspection date. If the State suspects fraud or other abuse, or in the event of an emergency, the State is not obligated to provide any prior notice.

d. Contractor shall pay for all costs and expenses of any audit or inspection which reveals information that, in the sole determination of the State, is sufficient to constitute a breach by the Contractor under this Contract. The Contractor will remit full payment to the State for such audit or inspection no later than 30 days after receiving an invoice from the State. If the State does not receive payment within such time, the State may setoff the amount from any moneys which the State would otherwise be obligated to pay the Contractor in accordance with this Contract.

e. Contractor shall keep and preserve or cause to be kept and preserved all of its and Contractor Parties' Records until three (3) years after the latter of (1) final payment under this Contract, or (2) the expiration or earlier termination of this Contract, as the same may be modified for any reason. The State may request an audit or inspection at any time during this period. If any Claim or audit

is started before the expiration of this period, the Contractor shall retain or cause to be retained all Records until all Claims or audit findings have been resolved.

f. Contractor shall cooperate fully with the State and its agents in connection with an audit or inspection. Following any audit or inspection, the State may conduct and the Contractor shall cooperate with an exit conference.

g. Contractor shall incorporate this entire Section verbatim into any contract or other agreement that it enters into with any Contractor Party.

17. Campaign Contribution Restriction

For all State contracts, defined in section 9-612 of the Connecticut General Statutes as having a value of $50,000 or more, or a combination or series of such agreements or contracts having a value of $100,000 or more in a calendar year, the authorized signatory to this Contract represents that they have received the State Elections Enforcement Commission's notice advising state contractors of state campaign contribution and solicitation prohibitions, and will inform its principals of the contents of the notice

18. Protection of Confidential Information

a. Contractor and Contractor Parties have a duty to and shall, at their own expense, protect from a Confidential Information Breach any and all Confidential Information which they come to possess or control, wherever and however stored or maintained, in a commercially reasonable manner in accordance with the highest current industry standards and best practices, as they may be amended from time to time.

b. Contractor and all Contractor Parties shall develop, implement and maintain a comprehensive written information security policy for the protection of Confidential Information that meets or exceeds current industry standards and best practices as they may be amended from time to time. The safeguards contained in the written information security policy must meet or exceed the standards for the protection of Confidential Information, and information of a similar character, as set forth in all applicable federal and State law and in written policy of the Client Agency or DAS concerning the confidentiality of Confidential Information. Such data-security program shall include, but not be limited to, the following:

   1. A security policy for employees related to the storage, access and transportation of data containing Confidential Information;

   2. Reasonable restrictions on access to records containing Confidential Information, including access to any locked storage where such records are kept and an auditable electronic system of logging and tracking the viewing, accessing or both of Confidential Information;

   3. A process for reviewing policies and security measures at least annually;

   4. Creating secure access controls to Confidential Information, including but not limited to passwords; and

   5. Encrypting of Confidential Information that is stored on laptops, portable devices and storage media or that is being transmitted electronically.

c. Contractor and Contractor Parties shall notify DAS, the Client Agency and the Connecticut Office of the Attorney General as soon as practical, but no later than the next Business Day, after they become aware of or suspect that any Confidential Information which Contractor or Contractor Parties have come to possess or control has been subject to a Confidential Information Breach. If a Confidential Information Breach has occurred which, in the sole opinion of the Client Agency after consultation with the Attorney General, constitutes a breach of security as defined in Connecticut General Statutes, § 36a- 701b, or otherwise (Breach), the Contractor shall, within three (3) Business Days after the notification, present a credit monitoring and protection plan to the Commissioner of DAS, the Client Agency, and the Connecticut Office of the Attorney General,

for review and approval. Such credit monitoring and protection plan shall be made available by the Contractor at its own cost and expense to all individuals affected by the Confidential Information Breach. Such credit monitoring or protection plan shall include, but is not limited to, reimbursement for the cost of placing and lifting one (1) security freeze per credit file pursuant to Connecticut General Statutes § 36a-701a. Such credit monitoring or protection plans shall be approved by the State in accordance with this Section and shall cover a length of time commensurate with the circumstances of the Breach. Neither Contractor's nor any Contractor Party's costs and expenses for the credit monitoring and protection plan shall be recoverable from DAS, the Client Agency, or any State of Connecticut entity or any affected individuals and shall be outside of any liability cap or limitation contained in this Contract.

d. Contractor shall incorporate the requirements of this Section in all subcontracts requiring each Contractor Party to safeguard Confidential Information in the same manner as provided for in this Section.

e. Nothing in this Section shall supersede in any manner Contractor's or Contractor Party's obligations pursuant to the provisions of this Contract concerning the obligations of the Contractor to the Client Agency or DAS.

19. Executive Orders and Other Enactments

a. All references in this Contract to any Federal, State, or local law, statute, public or special act, executive order, ordinance, regulation or code (collectively, "Enactments") shall mean Enactments that apply to the Contract at any time during its Term, or that may be made applicable to the Contract during its Term. This Contract shall always be read and interpreted in accordance with the latest applicable wording and requirements of the Enactments. Unless otherwise provided by Enactments, the Contractor is not relieved of its obligation to Perform under this Contract if it chooses to contest the applicability of the Enactments or the State's authority to require compliance with the Enactments.

b. This Contract is subject to the provisions of Executive Order No. Three of Governor Thomas J. Meskill, promulgated June 16, 1971, concerning labor employment practices, Executive Order No. Seventeen of Governor Thomas J. Meskill, promulgated February 15, 1973, concerning the listing of employment openings and Executive Order No. Sixteen of Governor John G. Rowland promulgated August 4, 1999, concerning violence in the workplace, all of which are incorporated into and are made a part of this Contract as if they had been fully set forth in it.

c. This Contract may be subject to (1) Executive Order No. 14 of Governor M. Jodi Rell, promulgated April 17, 2006, concerning procurement of cleaning products and services; and (2) Executive Order No. 61 of Governor Dannel P. Malloy promulgated December 13, 2017 concerning the Policy for the Management of State Information Technology Projects, as issued by the Office of Policy and Management, Policy ID IT-SDLC-17-04. If any of the Executive Orders referenced in this subsection is applicable, it is deemed to be incorporated into and made a part of this Contract as if fully set forth in it.

20. Non-Discrimination

a. For purposes of this Section, the following terms are defined as follows:

1. "Commission" means the Commission on Human Rights and Opportunities;

2. "Contract" and "contract" include any extension or modification of the Contract or contract;

3. "Contractor" and "contractor" include any successors or assigns of the Contractor or contractor;

4. "Gender identity or expression" means a person's gender-related identity, appearance or behavior, whether or not that gender-related identity, appearance or behavior is different from that traditionally associated with the person's physiology or assigned sex at birth,

which gender-related identity can be shown by providing evidence including, but not limited to, medical history, care or treatment of the gender-related identity, consistent and uniform assertion of the gender-related identity or any other evidence that the gender-related identity is sincerely held, part of a person's core identity or not being asserted for an improper purpose;

5. “good faith" means that degree of diligence which a reasonable person would exercise in the performance of legal duties and obligations;
6. "good faith efforts" shall include, but not be limited to, those reasonable initial efforts necessary to comply with statutory or regulatory requirements and additional or substituted efforts when it is determined that such initial efforts will not be sufficient to comply with such requirements;
7. "marital status" means being single, married as recognized by the state of Connecticut, widowed, separated or divorced;
8. "mental disability" means one or more mental disorders, as defined in the most recent edition of the American Psychiatric Association's "Diagnostic and Statistical Manual of Mental Disorders", or a record of or regarding a person as having one or more such disorders;
9. "minority business enterprise" means any small contractor(1) fifty-one per cent or more of the capital stock, if any, or assets of which are owned by a person or persons who (a) exercise operational authority over the daily affairs of the enterprise, (b) have the power to direct the management and policies and receive the beneficial interest of the enterprise, (c) possess managerial and technical competence and experience directly related to the principal business activities of the enterprise, and (d) are members of a minority, as defined in C.G.S. § 32-9n, or are individuals with a disability, or (2) which is a nonprofit corporation in which fifty-one per cent or more of the persons who exercise operational authority over the enterprise, (a) possess managerial and technical competence and experience directly related to the principal business activities of the enterprise, (b) have the power to direct the management and policies of the enterprise, and (c) are member of a minority, as defined in C.G.S. § 32-9n, or are individuals with a disability ; and
10. "public works contract" means any agreement (A) for construction, rehabilitation, conversion, extension, demolition or repair of changes or improvements in real property, and (B) that is financed in whole or in part by the State, including, but not limited to, matching expenditures, grants, loans, insurance or guarantees where such funding equals one hundred fifty thousand dollars or more.

For purposes of this Section, the terms “Contract” and “contract” do not include a contract where each contractor is (1) a political subdivision of the state, including, but not limited to, a municipality, unless the contract is a public works contract , (2) any other state, including but not limited to any federally recognized Indian tribal governments, as defined in C.G.S. § 1-267, (3) the federal government, (4) a foreign government, or (5) an agency of a subdivision, state or government described in the immediately preceding enumerated items (1), (2), (3),or (4).

b. (1) The Contractor agrees and warrants that in the performance of the Contract such Contractor will not discriminate or permit discrimination against any person or group of persons on the grounds of race, color, religious creed, age, marital status, national origin, ancestry, sex, sexual orientation, gender identity or expression, status as a veteran, status as a victim of domestic violence, status as a victim of sexual assault or status as a victim of trafficking in persons, intellectual disability, mental disability or physical disability, including, but not limited to, blindness, unless it is shown by such Contractor that such disability prevents performance of the work involved, in any manner prohibited by the laws of the United States or of the State of Connecticut; and the Contractor further agrees to take affirmative action to ensure that applicants with job-related qualifications are employed and that employees are treated when employed without

regard to their race, color, religious creed, age, marital status, national origin, ancestry, sex, gender identity or expression, sexual orientation, status as a veteran, status as a victim of domestic violence, status as a victim of sexual assault or status as a victim of trafficking in persons, intellectual disability, mental disability or physical disability, including, but not limited to, blindness, unless it is shown by the Contractor that such disability prevents performance of the work involved; (2) the Contractor agrees, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, to state that it is an "affirmative action equal opportunity employer" in accordance with regulations adopted by the Commission; (3) the Contractor agrees to provide each labor union or representative of workers with which the Contractor has a collective bargaining agreement or other contract or understanding and each vendor with which the Contractor has a contract or understanding, a notice to be provided by the Commission, advising the labor union or workers' representative of the Contractor's commitments under this section and to post copies of the notice in conspicuous places available to employees and applicants for employment; (4) the Contractor agrees to comply with each provision of this Section and Connecticut General Statutes §§ 46a-68e and 46a-68f and with each regulation or relevant order issued by said Commission pursuant to Connecticut General Statutes §§ 46a-56, 46a-68e, 46a-68f and 46a-86; and (5) the Contractor agrees to provide the Commission with such information requested by the Commission, and permit access to pertinent books, records and accounts, concerning the employment practices and procedures of the Contractor as relate to the provisions of this Section and Connecticut General Statutes § 46a-56. If the contract is a public works contract, the Contractor agrees and warrants that he or she will make good faith efforts to employ minority business enterprises as subcontractors and suppliers of materials on such public works projects.

c. Determination of the Contractor's good faith efforts shall include, but shall not be limited to, the following factors: The Contractor's employment and subcontracting policies, patterns and practices; the timing and value of bids; affirmative advertising, recruitment and training; technical assistance activities and such other reasonable activities or efforts as the Commission may prescribe that are designed to ensure the participation of minority business enterprises in public works projects.

d. The Contractor shall develop and maintain adequate documentation, in a manner prescribed by the Commission, of its good faith efforts.

e. The Contractor shall include the provisions of subsection (b) of this Section in every subcontract or purchase order entered into in order to fulfill any obligation of a contract with the State and in every subcontract entered into in order to fulfill any obligation of a public works contract, and such provisions shall be binding on a subcontractor, vendor or manufacturer unless exempted by regulations or orders of the Commission. The Contractor shall take such action with respect to any such subcontract or purchase order as the Commission may direct as a means of enforcing such provisions including sanctions for noncompliance in accordance with Connecticut General Statutes §46a-56; provided if such Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the Commission, the Contractor may request the State of Connecticut to enter into any such litigation or negotiation prior thereto to protect the interests of the State and the State may so enter.

f. The Contractor agrees to comply with the regulations referred to in this Section as they exist on the date of this Contract and as they may be adopted or amended from time to time during the term of this Contract and any amendments thereto.

g. Pursuant to subsection (c) of section 4a-60 of the Connecticut General Statutes, the Contractor, for itself and its authorized signatory of this Contract, affirms that it understands the obligations of this section and that it will maintain a policy for the duration of the Contract to assure that the Contract will be performed in compliance with the nondiscrimination requirements of such sections. The Contractor and its authorized signatory of this Contract demonstrate their understanding of this obligation by (A) having provided an affirmative response in the required

online bid or response to a proposal question which asks if the contractor understands its obligations under such sections, (B) signing this Contract, or (C) initialing this nondiscrimination affirmation **here in the following box**: ☐

21. Artificial Intelligence

a. During the Term, Contractor shall respond to Client Agency and DAS' information requests, no later than fifteen (15) Business Days from the date the Contractor receives a request, regarding (i) the use of Artificial Intelligence in any Deliverable or Performance by providing the data sets being collected and algorithms being used by the Contractor relating to such use, and (ii) the ongoing monitoring, assessment protocol and tools used by Contractor relating to the Artificial Intelligence used in any Deliverable or Performance. Contractor's response and data shall be delivered in a format acceptable to the Client Agency or DAS, as applicable.

b. If during the Term Contractor introduces Artificial Intelligence functionality into a Deliverable or any portion of a Deliverable that was not originally included in the Deliverables or Performance, Contractor shall provide DAS and the Client Agency the option, in DAS and Client Agency's sole discretion, to opt in or opt out of that Artificial Intelligence. Contractor shall not implement any such Artificial Intelligence without DAS' and the Client Agency's prior express written authority. Notwithstanding the foregoing, Contractor shall, no later than fifteen (15) Business Days after receiving a written request from DAS or the Client Agency, provide Artificial Intelligence functionality including, but not limited to, data sources and algorithms for any Deliverable or Performance.

c. No Artificial Intelligence used in a Deliverable or Performance shall (i) result in any unlawful discrimination against any individual or group of individuals, or (ii) have any unlawful disparate impact on any individual or group of individuals on the basis of any actual or perceived differentiating characteristic, including, but not limited to, age, genetic information, color, ethnicity, race, creed, religion, national origin, ancestry, sex, gender identity or expression, sexual orientation, marital status, familial status, pregnancy, veteran status, status as a victim of domestic violence, intellectual disability, mental disability or physical disability, including but not limited to blindness, or lawful source of income.

d. The Contractor may fulfill Artificial Intelligence disclosure obligations by providing one or more of the following items of non-source level information as specified by the Client Agency (a) summary-level information describing the purpose and use of the Artificial Intelligence; (b) functional summaries explaining the Artificial Intelligence tasks performed and the general nature of the Artificial Intelligence inputs and outputs; (c) high-level descriptions of Artificial Intelligence data sources identifying general categories of data used; (d) Artificial Intelligence training inputs described at a general level as to the type and source of the information used to train or refine the Artificial Intelligence; (e) Artificial Intelligence algorithmic logic explained conceptually as to how inputs are processed to generate Artificial Intelligence outputs; or (f) similar non-source level information as may be more specifically required by the Client Agency.

e. Nothing in this Section shall be construed to require the Contractor to disclose, transfer or provide access to any Contractor IP unless expressly agreed to in writing or as required by a court of competent jurisdiction.

22. Prohibition of Additional Terms of Use

The Contractor shall not require, as a condition of access to or use of any Deliverable under this Contract, that the State or its authorized Users agree to or be bound by any terms of use, service terms, privacy policy, click-through agreement, shrink-wrap agreement, browse-wrap agreement, or any other form of supplemental, unilateral or online terms, including without limitation, acknowledgment of third party licensing terms or additional disclaimers for third party components, products, content or open source software, or any other terms that conflict with the Master Agreement or Participating Addendum that are not already incorporated into this Contract (collectively, **"**Supplemental Terms**"**).

a. Any Supplemental Terms, whether presented before, during, or after delivery or access to or use of the Deliverables, are rejected and shall have no force or effect, regardless of any action or inaction of a User (including, but not limited to, clicking "I agree," opening a hyperlink, accessing a website, or continuing use of a service).

b. The Contractor may require the State or its Users to accept limitations on use only if those limitations are consistent with, all other terms of this Contract. No limitation on use shall be enforceable unless expressly previously agreed to in writing by the State. By way of example but not by limitation, acceptable limitations on use include restrictions on the use of the Licensed Software, including, without limitation: modifying, distributing or reverse engineering and other restrictions to ensure compliance with applicable laws and regulations and prevent illegal, harmful, or fraudulent activities or interference with system security. Acceptable limitations on use, by way of example but not limitation, do not include provisions regarding ownership or intellectual property rights or disclaimers.

c. Imposing, or any attempt to impose, Supplemental Terms on the State or its Users constitutes a material breach of this Contract. This provision is governed by Connecticut law and does not limit any right or remedy available to the State under Connecticut law or this Contract.

23. Health Insurance Portability and Accountability Act of 1996

a. If the Contractor is a Business Associate under the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as noted in this Contract, the Contractor must comply with all terms and conditions of this Section of the Contract. If the Contractor is not a Business Associate under HIPAA, this Section of the Contract does not apply to the Contractor for this Contract.

b. The Contractor is required to safeguard the use, publication and disclosure of information on all applicants for, and all clients who receive, services under the Contract in accordance with all applicable federal and state law regarding confidentiality, which includes but is not limited to HIPAA, more specifically with the Privacy and Security Rules at 45 C.F.R. Part 160 and Part 164, subparts A, C, and E.

c. The State of Connecticut Agency named on page 1 of this Contract ("Agency") is a "covered entity" as that term is defined in 45 C.F.R. § 160.103.

d. The Contractor is a "business associate" of the Agency, as that term is defined in 45 C.F.R. § 160.103.

e. The Contractor and the Agency agree to the following in order to secure compliance with the HIPAA, the requirements of Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), (Pub. L. 111-5, §§ 13400 to 13423), and more specifically with the Privacy and Security Rules at 45 C.F.R. Part 160 and Part 164, subparts A, C, D and E (collectively referred to herein as the "HIPAA Standards").

f. Definitions

1. "Breach" shall have the same meaning as the term is defined in section 45 C.F.R. 164.402 and shall also include a use or disclosure of PHI that violates the HIPAA Standards.

2. "Business Associate" shall mean the Contractor.

3. "Covered Entity" shall mean the Agency of the State of Connecticut named on page 1 of this Contract.

4. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R. § 164.501.

5. "Electronic Health Record" shall have the same meaning as the term is defined in section 13400 of the HITECH Act (42 U.S.C. §17921(5).

6. “Individual” shall have the same meaning as the term “individual”’ in 45 C.F.R. §160.103 and shall include a person who qualifies as a personal representative as defined in 45 C.F.R. § 164.502(g).
7. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.
8. “Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, and includes electronic PHI, as defined in 45 C.F.R. 160.103, limited to information created, maintained, transmitted or received by the Business Associate from or on behalf of the Covered Entity or from another Business Associate of the Covered Entity.
9. “Required by Law”’ shall have the same meaning as the term “required by law” in 45 C.F.R. § 164.103.
10. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.
11. “More stringent” shall have the same meaning as the term “more stringent” in 45 C.F.R. § 160.202.
12. “This Section of the Contract” refers to the HIPAA Provisions stated herein, in their entirety.
13. “Security Incident” shall have the same meaning as the term “security incident” in 45 CFR §164.304.
14. “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. part 160 and part 164, subpart A and C.
15. “Unsecured protected health information” shall have the same meaning as the term as defined in 45 C.F.R. 164.402.

g. Obligations and Activities of Business Associates.

1. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Section of the Contract or as Required by Law.
2. Business Associate agrees to use and maintain appropriate safeguards and comply with applicable HIPAA Standards with respect to all PHI and to prevent use or disclosure of PHI other than as provided for in this Section of the Contract and in accordance with HIPAA standards.
3. Business Associate agrees to use administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information that it creates, receives, maintains, or transmits on behalf of the Covered Entity.
4. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by Business Associate in violation of this Section of the Contract.
5. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Section of the Contract or any security incident of which it becomes aware.
6. Business Associate agrees, in accordance with 45 C.F.R. 502(e)(1)(ii) and 164.308(d)(2), if applicable, to ensure that any subcontractors that create, receive, maintain or transmit protected health information on behalf of the business associate, agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.
7. Business Associate agrees to provide access (including inspection, obtaining a copy or both),

at the request of the Covered Entity, and in the time and manner designated by the Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524. Business Associate shall not charge any fees greater than the lesser of the amount charged by the Covered Entity to an Individual for such records; the amount permitted by state law; or the Business Associate's actual cost of postage, labor and supplies for complying with the request.

8. Business Associate agrees to make any amendments to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the Covered Entity, and in the time and manner designated by the Covered Entity.

9. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created, maintained, transmitted or received by, Business Associate on behalf of Covered Entity, available to Covered Entity or to the Secretary in a time and manner agreed to by the parties or designated by the Secretary, for purposes of the Secretary investigating or determining Covered Entity's compliance with the HIPAA Standards.

10. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and section 13405 of the HITECH Act (42 U.S.C. § 17935) and any regulations promulgated thereunder.

11. Business Associate agrees to provide to Covered Entity, in a time and manner designated by the Covered Entity, information collected in accordance with subsection (g)(10) of this Section of the Contract, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and section 13405 of the HITECH Act (42 U.S.C. § 17935) and any regulations promulgated thereunder. Business Associate agrees at the Covered Entity's direction to provide an accounting of disclosures of PHI directly to an individual in accordance with 45 C.F.R. § 164.528 and section 13405 of the HITECH Act (42 U.S.C. § 17935) and any regulations promulgated thereunder.

12. Business Associate agrees to comply with any state or federal law that is more stringent than the Privacy Rule.

13. Business Associate agrees to comply with the requirements of the HITECH Act relating to privacy and security that are applicable to the Covered Entity and with the requirements of 45 C.F.R. §§ 164.504(e), 164.308, 164.310, 164.312, and 164.316.

14. In the event that an individual requests that the Business Associate

    A. restrict disclosures of PHI;

    B. provide an accounting of disclosures of the individual's PHI;

    C. provide a copy of the individual's PHI in an electronic health record; or

    D. amend PHI in the individual's designated record set the Business Associate agrees to notify the Covered Entity, in writing, within five business days of the request.

15. Business Associate agrees that it shall not, and shall ensure that its subcontractors do not, directly or indirectly, receive any remuneration in exchange for PHI of an Individual without

    A. The written approval of the covered entity, unless receipt of remuneration in exchange for PHI is expressly authorized by this Contract and

    B. The valid authorization of the individual, except for the purposes provided under section 13405(d)(2) of the HITECH Act, (42 U.S.C. § 17935(d)(2)) and in any accompanying regulations

16. Obligations in the Event of a Breach.

A. The Business Associate agrees that, following the discovery by the Business Associate or by a subcontractor of the Business Associate of any use or disclosure not provided for by this section of the Contract, any breach of unsecured protected health information, or any Security Incident, it shall notify the Covered Entity of such breach in accordance with Subpart D of Part 164 of Title 45 of the Code of Federal Regulations and this Section of the Contract.

B. Such notification shall be provided by the Business Associate to the Covered Entity without unreasonable delay, and in no case later than 30 days after the breach is discovered by the Business Associate, or a subcontractor of the Business Associate, except as otherwise instructed in writing by a law enforcement official pursuant to 45 C.F.R. 164.412. A breach is considered discovered as of the first day on which it is, or reasonably should have been, known to the Business Associate or its subcontractor. The notification shall include the identification and last known address, phone number and email address of each individual (or the next of kin of the individual if the individual is deceased) whose unsecured protected health information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such breach.

C. The Business Associate agrees to include in the notification to the Covered Entity at least the following information:

1. A description of what happened, including the date of the breach; the date of the discovery of the breach; the unauthorized person, if known, who used the PHI or to whom it was disclosed; and whether the PHI was actually acquired or viewed.

2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

3. The steps the Business Associate recommends that Individual(s) take to protect themselves from potential harm resulting from the breach.

4. A detailed description of what the Business Associate is doing or has done to investigate the breach, to mitigate losses, and to protect against any further breaches.

5. Whether a law enforcement official has advised the Business Associate, either verbally or in writing, that he or she has determined that notification or notice to Individuals or the posting required under 45 C.F.R. 164.412 would impede a criminal investigation or cause damage to national security and; if so, contact information for said official.

D. If directed by the Covered Entity, the Business Associate agrees to conduct a risk assessment using at least the information in subparagraphs 1 to 4, inclusive of (g) (16) (C) of this Section and determine whether, in its opinion, there is a low probability that the PHI has been compromised. Such recommendation shall be transmitted to the Covered Entity within 20 business days of the Business Associate's notification to the Covered Entity.

E. If the Covered Entity determines that there has been a breach, as defined in 45 C.F.R. 164.402, by the Business Associate or a subcontractor of the Business Associate, the Business Associate, if directed by the Covered Entity, shall provide all notifications required by 45 C.F.R. 164.404 and 45 C.F.R. 164.406.

F. Business Associate agrees to provide appropriate staffing and have established procedures to ensure that individuals informed of a breach have the opportunity to ask questions and contact the Business Associate for additional information regarding the

breach. Such procedures shall include a toll-free telephone number, an e-mail address, a posting on its Website and a postal address. Business Associate agrees to include in the notification of a breach by the Business Associate to the Covered Entity, a written description of the procedures that have been established to meet these requirements. Costs of such contact procedures will be borne by the Contractor.

G. Business Associate agrees that, in the event of a breach, it has the burden to demonstrate that it has complied with all notifications requirements set forth above, including evidence demonstrating the necessity of a delay in notification to the Covered Entity.

h. Permitted Uses and Disclosure by Business Associate.

1. General Use and Disclosure Provisions

Except as otherwise limited in this Section of the Contract, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Contract, provided that such use or disclosure would not violate the HIPAA Standards if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

2. Specific Use and Disclosure Provisions

A. Except as otherwise limited in this Section of the Contract, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

B. Except as otherwise limited in this Section of the Contract, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

C. Except as otherwise limited in this Section of the Contract, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

i. Obligations of Covered Entity.

1. Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity, in accordance with 45 C.F.R. § 164.520, or to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

2. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual(s) to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

3. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

j. Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Standards if done by the Covered Entity, except that Business Associate may use and disclose PHI for data aggregation, and management and administrative activities of Business Associate, as permitted under this Section of the Contract.

k. Term and Termination.

1. Term. The term of this Section of the Contract shall be effective as of the date the Contract is effective and shall terminate when the information collected in accordance with provision (g)(10) of this Section of the Contract is provided to the Covered Entity and all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
2. Termination for Cause Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
    A. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Contract if Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or
    B. Immediately terminate the Contract if Business Associate has breached a material term of this Section of the Contract and cure is not possible.
    C. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.
3. Effect of Termination.
    A. Except as provided in (k)(2) of this Section of the Contract, upon termination of this Contract, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity. Business Associate shall also provide the information collected in accordance with section (g)(10) of this Section of the Contract to the Covered Entity within ten business days of the notice of termination. This section shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.
    B. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon documentation by Business Associate that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Section of the Contract to such PHI and limit further uses and disclosures of PHI to those purposes that make return or destruction infeasible, for as long as Business Associate maintains such PHI. Infeasibility of the return or destruction of PHI includes, but is not limited to, requirements under state or federal law that the Business Associate maintains or preserves the PHI or copies thereof.

I. Miscellaneous Sections.

1. Regulatory References. A reference in this Section of the Contract to a section in the Privacy Rule means the section as in effect or as amended.
2. Amendment. The Parties agree to take such action as in necessary to amend this Section of the Contract from time to time as is necessary for Covered Entity to comply with requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104191.
3. Survival. The respective rights and obligations of Business Associate shall survive the termination of this Contract.
4. Effect on Contract. Except as specifically required to implement the purposes of this Section of the Contract, all other terms of the Contract shall remain in force and effect.
5. Construction. This Section of the Contract shall be construed as broadly as necessary to implement and comply with the Privacy Standard. Any ambiguity in this Section of the Contract shall be resolved in favor of a meaning that complies, and is consistent with, the

Privacy Standard.

6. Disclaimer. Covered Entity makes no warranty or representation that compliance with this Section of the Contract will be adequate or satisfactory for Business Associate's own purposes. Covered Entity shall not be liable to Business Associate for any claim, civil or criminal penalty, loss or damage related to or arising from the unauthorized use or disclosure of PHI by Business Associate or any of its officers, directors, employees, contractors or agents, or any third party to whom Business Associate has disclosed PHI contrary to the sections of this Contract or applicable law. Business Associate is solely responsible for all decisions made, and actions taken, by Business Associate regarding the safeguarding, use and disclosure of PHI within its possession, custody or control.

7. Indemnification. The Business Associate shall indemnify and hold the Covered Entity harmless from and against any and all claims, liabilities, judgments, fines, assessments, penalties, awards and any statutory damages that may be imposed or assessed pursuant to HIPAA, the HIPAA Standards, or the HITECH Act (all as amended), including, without limitation, attorney's fees, expert witness fees, costs of investigation, litigation or dispute resolution, and costs awarded thereunder, relating to or arising out of any violation by the Business Associate and its agents, including subcontractors, of any obligation of Business Associate and its agents, including subcontractors, under this Section of the Contract, under HIPAA, the HITECH Act, and the HIPAA Standards.

24. Iran Energy Investment Certification

a. Pursuant to Conn. Gen. Stat. § 4-252a, the Contractor certifies that it has not made a direct investment of twenty million dollars or more in the energy sector of Iran on or after October 1, 2013, as described in Section 202 of the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010, and has not increased or renewed such investment on or after said date.

b. If the Contractor makes a good faith effort to determine whether it has made an investment described in subsection (a) of this Section then the Contractor shall not be deemed to be in breach of the Contract or in violation of this Section. A "good faith effort" for purposes of this subsection includes a determination that the Contractor is not on the list of persons who engage in certain investment activities in Iran created by the Department of General Services of the state of California pursuant to Division 2, Chapter 2.7 of the California Public Contract Code. Nothing in this subsection shall be construed to impair the ability of the State or quasi-public agency to pursue a breach of contract action for any violation of the provisions of the Contract.

25. Large State Contract Representation for Contractor

Pursuant to Conn. Gen. Stat. § 4-252 and Acting Governor Susan Bysiewicz Executive Order No. 21-2, promulgated July 1, 2021, the Contractor, for itself and on behalf of all of its principals or key personnel who submitted a bid or proposal, represents:

(1) That no gifts were made by (A) the Contractor, (B) any principals and key personnel of the Contractor, who participate substantially in preparing bids, proposals or negotiating State contracts, or (C) any agent of the Contractor or principals and key personnel, who participates substantially in preparing bids, proposals or negotiating State contracts, to (i) any public official or State employee of the State agency or quasi- public agency soliciting bids or proposals for State contracts, who participates substantially in the preparation of bid solicitations or requests for proposals for State contracts or the negotiation or award of State contracts, or (ii) any public official or State employee of any other State agency, who has supervisory or appointing authority over such State agency or quasi-public agency;
(2) That no such principals and key personnel of the Contractor, or agent of the Contractor or of such principals and key personnel, knows of any action by the Contractor to circumvent such prohibition on gifts by providing for any other principals and key personnel, official, employee or agent of the Contractor to provide a gift to any such public official or State employee; and
(3) That the Contractor is submitting bids or proposals without fraud or collusion with any person.

26. Large State Contract Representation for Official or Employee of State Agency

Pursuant to Conn. Gen. Stat. § 4-252 and Acting Governor Susan Bysiewicz Executive Order No. 21-2, promulgated July 1, 2021, the State official or employee represents that the selection of the person, firm or corporation was not the result of collusion, the giving of a gift or the promise of a gift, compensation, fraud or inappropriate influence from any person.

27. Consumer Data Privacy and Online Monitoring

Pursuant to section 4e-72a of the Connecticut General Statutes, Contractor shall at all times comply with all applicable provisions of sections 42-515 to 42-525, inclusive, of the Connecticut General Statutes, as the same may be revised or modified.

28. Purchase Orders

a. This Contract itself is not an authorization for the Contractor to begin Performance in any way. The Contractor may begin Performance only after it has received a duly issued Purchase Order against this Contract for Performance.

b. The Client Agency shall issue a Purchase Order against this Contract directly to the Contractor and to no other party.

c. All Purchase Orders shall be in written or electronic form, bear the Contract number (if any) and comply with all other State and Client Agency requirements, particularly the Client Agency's requirements concerning procurement. Purchase Orders issued in compliance with such requirements shall be deemed to be duly issued.

d. A Contractor Performing without a duly issued Purchase Order in accordance with this Section does so at the Contractor's own risk.

e. The Client Agency may, in its sole discretion, deliver to the Contractor any or all duly issued Purchase Orders via electronic means only, such that the Client Agency shall not have any additional obligation to deliver to the Contractor a "hard copy" of the Purchase Order or a copy bearing any hand-written signature or other "original" marking.

29. Deliverable Evaluation, Acceptance and Ownership

a. If any Deliverable furnished by Contractor under the terms of this Contract is subject to User Acceptance Testing ("UAT"), then UAT for each Deliverable begins as of the date the Client Agency notifies the Contractor in writing that the Deliverable provided for UAT has been successfully delivered and/or installed in the development and testing computer environment and is ready for UAT. The following procedures will apply during UAT:

    1. The Client Agency shall provide Contractor with (a) written notice that the Deliverable was delivered and/or installed and ready for UAT or (b) a written statement which identifies in reasonable detail, with references to the applicable requirements, the deficiencies preventing delivery and/or installation.

    2. Contractor shall have five (5) Business Days, or such other period mutually agreed upon by the parties in writing, from the date it receives the notice of deficiencies to complete corrective actions to make the Deliverable conform in all material respects to the applicable Specifications. The Client Agency shall review the corrected Deliverable and notify Contractor in writing of completion of delivery and/or installation of the Deliverable or rejection in accordance with the foregoing provisions of this Section.

    3. The Acceptance Date for a Deliverable shall be the date of written notice of Acceptance of the Deliverable from Client Agency to Contractor in accordance with subsection b below.

b. After delivery and/or installation of each of the Deliverables required under the Contract, or a SOW, as applicable, the Client Agency shall perform UAT on the System. If the System has met the Acceptance Criteria during UAT, Client Agency shall implement the System in the Client

Agency's production environment. If UAT for the System is successfully completed, the Client Agency shall in writing notify the Contractor of the Client Agency's Acceptance of the System, and the date of such notice will be the Acceptance Date for the System.

c. If requested by Contractor, Client Agency shall complete Contractor's acceptance certificate, in a form reasonably acceptable to Client Agency, so long as such certificate does not amend, alter or modify in any way the terms of this Contract.

d. The State shall own all Deliverables provided by Contractor under this Contract, subject to subparagraph e) below, and shall have the right to alter, modify, create derivative works, copy and distribute any Deliverable acquired under this Contract including any and all configuration, programming, inventions or improvements to computer programs or base software or both, specifically developed by the Contractor and paid for by the Client Agency pursuant to this Contract. The State shall retain all ownership rights to any such configuration, programming, inventions or improvements.

    1. The State shall own any inventions or improvements to Contractor IP, if such invention or improvement was developed in the Performance of this Contract and paid for by the State. Contractor shall have a perpetual license at no cost to use any such inventions or improvements to Contractor IP for Contractor's own or commercial purposes.

    Nothing in this provision shall be construed as transferring to the State any ownership interest or rights to Contractor IP.

e. The State shall have a nonexclusive, nontransferable, perpetual license to use, alter, modify, create derivative works (without the right to sublicense) and copy Contractor IP in connection with the State's business needs and operations if Contractor IP is provided to the State by Contractor in order to Perform any Services or provide any Deliverables required under this Contract.

f. If any Deliverable becomes the actual or prospective subject of any patent, copyright, license or proprietary rights claim or proceeding, Contractor shall do one or more of the following at the option of Contractor:

    1. Modify the Deliverable or substitute another equally suitable Deliverable (provided that the function of the modified or substitute Deliverable equals or exceeds that of the original Deliverable);

    2. Obtain for the Client Agency the right to continued use of the Deliverable; or

    3. If neither 1 nor 2 above is commercially reasonable, Client Agency shall discontinue use of the Deliverable subject to such claim or proceeding and the Contractor shall refund the Client Agency the fees paid for the Deliverable.

g. Each party reserves for itself all proprietary rights not expressly granted to the other. Contractor shall not be limited in developing, using or marketing services or products which are similar to the Deliverables or Services provided under this Contract.

30. Risk of Loss

The State shall not be liable to Contractor for any risk of Deliverable loss or damage while Deliverables are in transit, or while in the Client Agency's possession, except when such loss or damage is due directly to the Client Agency's negligence or intentional misconduct. Nothing in this Section is intended nor shall it be construed, in any manner, as waiving or compromising the sovereign immunity of the State.

31. Background Checks

The Contractor and Contractor Parties shall submit to and incur the cost of fingerprint supported federal and state criminal history background checks as may be required by the State, the State of Connecticut Department of Emergency Services and Public Protection, or as provided for in any State document that governs procedures for background checks. The Contractor and Contractor Parties

shall cooperate fully as necessary or reasonably requested with the State and its agents in connection with such background checks.

32. Contractor Guaranties

a. Contractor shall:

1. Perform fully under this Contract;
2. Guarantee the Goods or Services against defective material or workmanship and to repair any damage or marring occasioned in transit or, at the Client Agency's option, replace them;
3. Furnish adequate protection from damage for all work and to repair damage of any kind, for which its workers are responsible, to the Site, Goods, the Contractor's work or that of Contractor Parties;
4. With respect to the provision of Services, pay for all permits, licenses and fees and give all required or appropriate notices; and
5. Adhere to all Contractual provisions ensuring the confidentiality of Records that the Contractor has access to and are exempt from disclosure under the State's Freedom of Information Act or other applicable law.

33. Contractor Responsibility

The Contractor shall be responsible for the entire Performance under this Contract regardless of whether the Contractor itself Performs. The Contractor shall be the sole point of contact concerning the management of this Contract, including Performance issues. The Contractor is solely and completely responsible for adherence by the Contractor Parties to all applicable provisions of this Contract.

34. Representations and Warranties

Contractor represents and warrants to the State for itself and, as applicable, the Contractor Parties that:

a. each is a duly and validly existing under the laws of each such entity's respective states of organization and authorized to conduct business in the State of Connecticut in the manner contemplated by this Contract. Further, as appropriate, each has taken all necessary action to authorize the execution, delivery and Performance of this Contract and have the power and authority to execute, deliver and Perform its obligations under this Contract;

b. each will comply with all applicable State and Federal laws and municipal ordinances in satisfying its obligations to the State under and pursuant to this Contract, including, but not limited to (1) Connecticut General Statutes Title 1, Chapter 10, concerning the State's Codes of Ethics; (2) Title 4a, Chapter 58 concerning State purchasing; and (3) Title 22a, Chapter 446c, section 22a-194a concerning the use of polystyrene foam;

c. the execution, delivery and Performance of this Contract will not violate, be in conflict with, result in a breach of or constitute (with or without due notice and/or lapse of time) a default under any of the following, as applicable: (1) any provision of law; (2) any order of any court or the State; or (3) any indenture, agreement, document or other instrument to which it is a party or by which it may be bound;

d. each is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any governmental entity;

e. as applicable, each has not, within the three years preceding the Effective Date of this Contract, in any of their current or former jobs, been convicted of, or had a civil judgment rendered against them or against any person who would Perform under this Contract, for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or Performing a transaction or contract with any governmental entity. This includes, but is not limited to, violation of federal or

state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records or property, making false statements, or receiving stolen property;

f. each is not presently indicted for or otherwise criminally or civilly charged by any governmental entity with commission of any of the offenses listed above;

g. they have notified DAS in writing whether they have had any contracts with any governmental entity Terminated for cause within the three (3) years preceding the Effective Date;

h. none has employed or retained any entity or person, other than a bona fide employee working solely for them, to solicit or secure this Contract and it has not paid or agreed to pay any entity or person, other than a bona fide employee working solely for them, any fee, commission, percentage, brokerage fee, gifts, or any other consideration contingent upon or resulting from the award or making of this Contract or any assignments made in accordance with the terms of this Contract;

i. to the best of each entity's knowledge, there are no Claims involving Contractor or Contractor Parties that might reasonably be expected to materially adversely affect their businesses, operations, assets, properties, financial stability, business prospects or ability to Perform fully under this Contract;

j. each shall disclose, to the best of its knowledge, to the State in writing any Claims involving it that would be required disclosure on Form 8-K of the Securities Exchange Act of 1934 no later than ten (10) calendar days after becoming aware or after it should have become aware of any such Claims. For purposes of the Contractor's obligation to disclose any Claims to the State, the ten (10) calendar days in the Section of this Contract concerning disclosure of Contractor Parties litigation shall run consecutively with the ten (10) days provided for in this representation and warranty;

k. each is able to Perform under this Contract using their own resources or the resources of a party who has not submitted a proposal;

l. if Contractor does not have plenary authority to make the representations and warranties in this Section, as applicable, on behalf of Contractor Parties, then Contractor shall enter into a written contract with Contractor Parties, in which contract Contractor Parties shall make all of the applicable representations and warranties in this Section;

m. each has paid all applicable workers' compensation second injury fund assessments concerning all previous work done in Connecticut; they have a record of compliance with Occupational Health and Safety Administration regulations without any unabated, willful or serious violations;

n. none owes unemployment compensation contributions;

o. none is delinquent in the payment of any taxes owed, or, that they have filed a sales tax security bond, and they have, if and as applicable, filed for motor carrier road tax stickers and have paid all outstanding road taxes;

p. all of each entity's vehicles have current registrations and, unless such vehicles are no longer in service, they shall not allow any such registrations to lapse;

q. each Contractor Party has vested in the Contractor plenary authority to bind the Contractor Parties to the full extent necessary or appropriate to ensure full compliance with and Performance in accordance with all of the terms of this Contract and that all appropriate parties shall also provide, no later than fifteen (15) days after receiving a request from DAS or the Client Agency, such information as DAS or the Client Agency may require to evidence, in their sole determination, compliance with this Section;

r. each either owns or has the authority to use all the Deliverables;

s. to the best knowledge of Contractor, the Deliverables do not infringe or misappropriate any patent, copyright, trade secret or other intellectual property right of a third party;

t. to the best knowledge of Contractor, the Client Agency's use of any Deliverables in a manner consistent with this Contract shall not infringe or misappropriate any patent, copyright, trade secret or other intellectual property right of a third party;

u. if any party shall procure any Deliverables, they shall sublicense such Deliverables and the Client Agency shall be afforded the full benefits of any manufacturer or subcontractor licenses for the use of the Deliverables; and

v. each shall assign or otherwise transfer to the Client Agency or afford the Client Agency the full benefits of any manufacturer's warranty for the Deliverables, to the extent that such warranties are assignable or otherwise transferable to the Client Agency.

35. Contractor Changes

The Contractor shall notify DAS in writing no later than ten (10) days from the effective date of any change in:

a. its certificate of incorporation or other organizational document;

b. more than a controlling interest in the ownership of the Contractor; or

c. the individual(s) in charge of the Performance.

This change shall not relieve the Contractor of any responsibility for the accuracy and completeness of the Performance. DAS, after receiving written notice by the Contractor of any such change, may require such agreements, releases and other instruments evidencing, to DAS' satisfaction, that any individuals retiring or otherwise separating from the Contractor have been compensated in full or that provision has been made for compensation in full, for all work performed under terms of this Contract. The Contractor shall deliver such documents to DAS in accordance with the terms of DAS' written request. DAS may also require, and the Contractor shall deliver, a financial statement showing that solvency of the Contractor is maintained. The death of any Contractor Party, as applicable, shall not release the Contractor from the obligation to Perform under this Contract; the surviving Contractor Parties, as appropriate, must continue to Perform under this Contract until Performance is fully completed.

36. Continued Performance

The Contractor and Contractor Parties shall continue to Perform their obligations under this Contract while any dispute concerning this Contract is being resolved.

37. Representations and Warranties Regarding Motor Vehicles

If in the course of Performance or in any other way related to this Contract the Contractor at any time uses or operates "motor vehicles," as that term is defined by Conn. Gen. Stat. §14-1 (including, but not limited to such services as snow plowing, sanding, hauling or delivery of materials, freight or merchandise, or the transportation of passengers), then the Contractor, represents and warrants for itself and the Contractor Parties, that:

a. it is the owner of record or lessee of record of each such motor vehicle used in the Performance of this Contract, and each such motor vehicle is duly registered with the Connecticut Department of Motor Vehicles ("ConnDMV") in accordance with the provisions of Chapter 246 of the Connecticut General Statutes. Each such registration shall be in valid status, and shall not be expired, suspended or revoked by ConnDMV, for any reason or cause. If such motor vehicle is not registered with ConnDMV, then it shall be duly registered with another state or commonwealth in accordance with such other state's or commonwealth's applicable statutes. Each such registration shall be in valid status, and shall not be expired, suspended or revoked by such other state or commonwealth for any reason or cause.

b. each such motor vehicle shall be fully insured in accordance with the provisions of Sections 14-12b, 14-112 and 38a-371 of the Connecticut General Statutes, as amended, in the amounts required by the said sections or in such higher amounts as have been specified by ConnDMV as

a condition for the award of this Contract, or in accordance with all substantially similar provisions imposed by the law of the jurisdiction where the motor vehicle is registered.

c. each Contractor Party who uses or operates a motor vehicle at any time in the Performance of this Contract shall have and maintain a motor vehicle operator's license or commercial driver's license of the appropriate class for the motor vehicle being used or operated. Each such license shall bear the endorsement or endorsements required by the provisions of Section 14-36a of the Connecticut General Statutes, as amended, to operate such motor vehicle, or required by substantially similar provisions imposed by the law of another jurisdiction in which the operator is licensed to operate such motor vehicle. The license shall be in valid status, and shall not be expired, suspended or revoked by ConnDMV or such other jurisdiction for any reason or cause.

d. each motor vehicle shall be in full compliance with all of the terms and conditions of all provisions of the Connecticut General Statutes and regulations, or those of the jurisdiction where the motor vehicle is registered, pertaining to the mechanical condition, equipment, marking and operation of motor vehicles of such type, class and weight, including, but not limited to, requirements for intrastate carriers with motor vehicles having a gross vehicle weight rating or gross combination weight rating or gross vehicle weight or gross combination weight of 18,001 pounds or more or interstate carriers with motor vehicles having a gross vehicle weight rating or gross combination weight rating or gross vehicle weight or gross combination weight of 10,001 pounds or more otherwise described by the provisions of Conn. Gen. Stat. § 14-163c(a) and all applicable provisions of the Federal Motor Carrier Safety Regulations, as set forth in Title 49, Parts 382 to 399, inclusive, of the Code of Federal Regulations. If the Contractor is a "motor carrier," as that term is defined in section 49 CFR Part 390, and the Contractor is subject to an order issued by the Federal Motor Carrier Safety Administration that prohibits such Contractor from operating or allowing the operation of a motor vehicle, then the Contractor shall comply fully with such order. In addition, if a motor vehicle or its operator is declared out of service pursuant to Conn. Gen. Stat. § 14-163c(d)(4), then the Contractor shall not operate or allow the operation of that motor vehicle and shall not allow the operator to operate a motor vehicle while the respective subject out-of-service order is in effect.

38. Call Center and Customer Service Work

Pursuant to Conn. Gen. Stat. §31-57aa(h), Contractor shall Perform all required State business-related call center and customer service work entirely within the state of Connecticut. If Contractor Performs work outside of the state of Connecticut and adds customer service employees who will Perform work pursuant to this Contract, then Contractor shall employ such new employees within the state of Connecticut prior to any such employee Performing any work pursuant to this Contract.

39. Tangible Personal Property

a. Contractor on its behalf and on behalf of its Affiliates, as defined below, shall comply with the provisions of Conn. Gen. Stat. §12-411b, as follows:

1. For the Term, Contractor and its Affiliates shall collect and remit to the State of Connecticut, Department of Revenue Services, any Connecticut use tax due under the provisions of Chapter 219 of the Connecticut General Statutes for items of tangible personal property sold by the Contractor or by any of its Affiliates in the same manner as if the Contractor and such Affiliates were engaged in the business of selling tangible personal property for use in Connecticut and had sufficient nexus with the State under the provisions of Chapter 219 to be required to collect Connecticut use tax;

2. A customer's payment of a use tax to the Contractor or its Affiliates relieves the customer of liability for the use tax;

3. Contractor and its Affiliates shall remit all use taxes they collect from customers on or before the due date specified in this Contract if any, which may not be later than the last day of the month next succeeding the end of a calendar quarter or other tax collection period during which the tax was collected;

4. Contractor and its Affiliates are not liable for use tax billed by them but not paid to them by a customer; and

5. Any Contractor or Affiliate who fails to remit use taxes collected on behalf of its customers by the due date specified in this Contract shall be subject to the interest and penalties provided for persons required to collect sales tax under Chapter 219 of the Connecticut General Statutes.

b. For purposes of this Section of this Contract, the word “Affiliate” means any person, as defined in section 12-1 of the Connecticut General Statutes, that controls is controlled by, or is under common control with another person. A person controls another person if the person owns, directly or indirectly, more than ten percent of the voting securities of the other person. The term “voting security” means a security that confers upon the holder the right to vote for the election of members of the board of directors or similar governing body of the business, or that is convertible into, or entitles the holder to receive, upon its exercise, a security that confers such a right to vote. “Voting security” includes a general partnership interest.

Contractor represents and warrants that each of its Affiliates has vested in the Contractor plenary authority to so bind the Affiliates in any agreement with the State of Connecticut. Contractor on its own behalf and on behalf of its Affiliates shall also provide, no later than 30 days after receiving a request by the State’s contracting authority, such information as the State may require to ensure, in the State’s sole determination, compliance with the provisions of Chapter 219 of the Connecticut General Statutes, including, but not limited to, §12-411b

40. Advertising

The Contractor shall not refer to sales to the State for advertising or promotional purposes, including, but not limited to, posting any material or data on the Internet, without DAS’ prior written approval.

41. Confidentiality; Non-Disclosure

The State shall exercise at least the same degree of care to safeguard any trade secrets or confidential information of Contractor as the State does its own property of a similar nature and shall take reasonable steps to ensure that neither the confidential information of Contractor nor any part of it will be disclosed for reasons other than its own business interests. Such prohibition on disclosures does not apply to disclosures by the State to its employees, agents or representatives, provided such disclosures are reasonably necessary to the State’s use of the Deliverable, and provided further that the State will take all reasonable steps to ensure that the Deliverable is not disclosed by such parties in contravention of this Contract. The State’s performance of the requirements of this Section shall be subject to the State of Connecticut Freedom of Information Act ("FOIA").

All Records, Client Agency Data, and any Data owned by the State in any form, in the possession of the Contractor or Contractor Parties, whether uploaded, collected, stored, held, hosted, located or utilized by Contractor and Contractor Parties directly or indirectly, must remain within the continental United States.

42. Assignment

The Contractor shall not assign any of its rights or obligations under this Contract, voluntarily or otherwise, in any manner without the prior written consent of DAS. DAS may void any purported assignment in violation of this Section and declare the Contractor in breach of Contract. Any Termination by DAS for a breach is without prejudice to DAS’ or the State’s rights or possible Claims.

43. Americans with Disabilities Act

Contractor represents that it and Contractor’s Performance complies, and during the Term, shall comply with the Americans with Disabilities Act of 1990, as amended, 42 U.S.C. §§12101 et seq, and with all other applicable federal and State laws concerning accessibility and nondiscrimination on the basis of disability. Failure of Contractor to satisfy this standard either now or during the Term constitutes a material breach of the Contract and entitles the State to exercise all remedies available

under the Contract, the law and in equity. Contractor shall indemnify, defend and hold the State harmless from any liability that may be imposed upon the State as a result of any failure of Contractor to be in compliance with the Americans with Disabilities Act.

44. Accessibility

a. The Contractor shall ensure that all Deliverables provided under this Contract comply with all applicable federal and State accessibility laws and standards, including, without limitation, the Americans with Disabilities Act of 1990, as amended (ADA); section 504 and section 508 of the Rehabilitation Act of 1973; the Connecticut General Statutes; the State of Connecticut Accessibility & Inclusivity Policy for Websites and Digital Assets, which is found at the following link: State of Connecticut Digital Accessibility Policy; and the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, which is found at the following link: https://www.w3.org/TR/WCAG21/ or any successor standard adopted by the State during the Term.

b. No later than 10 Business Days after receiving the State's written request or as specified in a Statement of Work, the Contractor shall provide accessibility documentation demonstrating the Deliverables' accessibility compliance, including, without limitation, the Accessibility Conformance Report (ACR) using the then current WCAG Voluntary Product Accessibility Template (VPAT) standards located at https://www.itic.org/policy/accessibility/vpat. Such documentation demonstrating accessibility compliance may be subject to disclosure under the Connecticut Freedom of Information Act, Conn. Gen. Stat. §§ 1-200, et seq. The Contractor shall cooperate fully with the State in responding to any FOIA request concerning accessibility compliance, and providing such information and delivering any instruments, documents and materials and take such other actions as the State may deem to be necessary or appropriate in order to comply fully as may be required pursuant to the FOIA.

c. The Contractor shall also deliver an ACR every twelve (12) months beginning on the first anniversary of the Effective Date and continuing for the duration of the Term. The Contractor shall deliver such ACR for the Deliverables using the WCAG VPAT version in effect at the time of delivery.

d. The Contractor shall maintain the Deliverables in continuous compliance with applicable accessibility requirements throughout the Term. If at any time during the Term, the Deliverables do not comply with the applicable accessibility requirements, Contractor shall, at no cost to the State, remediate the noncompliance within the time period specified by the State. The Contractor shall not be responsible for noncompliance resulting from the State's unauthorized use of, or material modification to, the Deliverables.

e. The State's rights under this Section are cumulative and in addition to, and not in limitation of, any other rights or remedies available to the State under this Contract, at law, or in equity, including the right to require remediation, withhold payment, terminate for cause, seek indemnification, or pursue injunctive or equitable relief.

f. Nothing in this Section requires the Contractor to disclose, transfer, or provide access to any Contractor IP unless expressly agreed to in writing or disclosure is required by a court of competent jurisdiction.

45. Environmentally Preferable Products

a. If Contractor is providing Environmentally Preferable products (EPP) under this Contract, then, as to those products only, the Contractor shall throughout the Term: (1) maintain those Deliverables in continuous compliance with applicable EPP standards or guidelines as identified in the Solicitation and in Exhibit A, Deliverables; (2). use products that are energy-efficient, water-efficient, recycled-content, recyclable, biodegradable, low-toxicity, avoid known health risks, conserve natural resources, or are otherwise environmentally preferable, as applicable; and (3) minimize environmental impacts associated with packaging, transportation, use and disposal.

b. No later than 10 Business Days after receiving the State's written request, Contractor shall deliver documentation validating that products represented as EPP comply with EPP standards, which documentation may include manufacturer certifications or product specifications. The State shall review the documentation and notify the Contractor whether it has or has not approved the form and content of such documentation validating EPP compliance. If the State determines not to approve the documentation, then the State shall in its notification to Contractor, explain the deficiencies in the documentation and identify the modifications or additions to the documentation that are necessary for the State to approve the documentation. The process of delivery by the Contractor and review by the State of the documentation continues until the State approves the documentation.

46. Consulting Agreements Representation

Pursuant to Conn. Gen. Stat. § 4a-81, the person signing this Contract on behalf of the Contractor represents, to their best knowledge and belief and subject to the penalty of false statement as provided in Conn. Gen. Stat. § 53a-157b, that the Contractor has not entered into any consulting agreements in connection with this Contract, except for the agreement(s) described in Attachment A. "Consulting agreement" means any written or oral agreement to retain the services, for a fee, of a consultant for the purposes of (A) providing counsel to a contractor, vendor, consultant or other entity seeking to conduct, or conducting, business with the State, (B) contacting, whether in writing or orally, any executive, judicial, or administrative office of the State, including any department, institution, bureau, board, commission, authority, official or employee for the purpose of solicitation, dispute resolution, introduction, requests for information, or (C) any other similar activity related to such contracts. "Consulting agreement" does not include any agreements entered into with a consultant who is registered under the provisions of chapter 10 of the Connecticut General Statutes as of the date such contract is executed in accordance with the provisions of Conn. Gen. Stat. §4a-81.

Attachment A – Consulting Agreements Representation

Instructions: Complete all fields in the space provided, include additional forms as applicable.

1. Consultant and Firm Information

Consultant's Full Name and Professional Title:

Click or tap here to enter text.

Name of firm, if applicable:

Click or tap here to enter text.

2. Consultant Agreement Details

Start Date: Click or tap to enter a date.

End Date: Click or tap to enter a date.

Cost – Enter total cost or fee: Click or tap here to enter text.

3. Basic Terms of the Consulting Agreement

Click or tap here to enter text.

4. Description of Services Provided

Click or tap here to enter text.

5. Former State Employee or Public Official Disclosure

Is the consultant a former State of Connecticut employee or former public official?

☐ Yes ☐ No

If yes: Enter name of former state agency. Leave blank if the answer above is No.

Click or tap here to enter text.

If yes: Enter termination date of employment: Click or tap to enter a date.

EXHIBIT 3

Minimum Service Level Requirements

This Exhibit 3 establishes minimum performance standards applicable to all Services provided under this Contract. Each Statement of Work (SOW) may supplement, modify, or replace specific metrics and thresholds defined herein.

1. **Definitions**

As used in this Exhibit 3, the following definitions shall have the following meanings:

A. Available Time means 24 hours × number of days in the month.

B. Downtime means any period, measured in minutes, during which the hosted services are not available to Client Agency or its Users in accordance with agreed performance standards, excluding Excluded Unavailability.

C. Excluded Unavailability means downtime resulting from:
(a) scheduled maintenance windows approved by the Client Agency;
(b) force majeure events, as defined in Section XIV.7 (Force Majeure) of Attachment A (NASPO ValuePoint Master Agreement Terms and Conditions of Exhibit 1 (Master Agreement);
(c) failures of systems or networks not under Contractor control; or
(d) downtime approved by Client Agency for major upgrades.

D. Incident means any unplanned interruption or degradation of the hosted services.

E. Severity Level means the categorization of an Incident according to business impact, as further described below.

F. System Availability means the percentage of total time during which the hosted services are operational and accessible to Client Agency and its Users, excluding Excluded Unavailability.

G. System Reliability means the ability of the System to operate continuously and Perform as designed under normal conditions.

2. **Minimum Service Level Requirements**

A. System Availability.

Contractor shall maintain System Availability as defined in the applicable SOW. Each SOW shall define the specific uptime percentage, related performance standards, and any applicable remedies for failure to meet those requirements. The below subparagraphs B – E set forth the minimum requirements applicable to each SOW.

B. Calculation.

System Availability = (Available Time – Downtime) / Available Time × 100.

C. Scheduled Downtime.

Contractor shall provide at least ten (10) Business Days' advance notice of any scheduled downtime. Such downtime must be (1) pre-approved by Client Agency, (2) limited to reasonable duration, and (3) scheduled during off-peak hours unless otherwise agreed. For major upgrades or Improvements requiring extended Downtime, the Parties shall mutually establish substitute timeframes.

D. Reporting and Monitoring.

Contractor shall maintain automated monitoring of System Availability and furnish availability reports as defined in each SOW.

Each SOW shall specify the frequency (e.g., daily, weekly, monthly) and content of such reports.

Failure to meet the System Availability requirement will trigger the remedies in Section 6.

E. System Reliability and Resilience.

Contractor shall host and maintain the System to ensure continuous operability for productive Client Agency use. At a minimum, Contractor shall:

i. Maintain redundant hosting or disaster-recovery infrastructure located in geographically separate U.S. data centers; and
ii. Perform automated daily and weekly data backups of production and configuration data. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) shall be defined in the applicable SOW.

3. **System Maintenance and Support**

A. Contractor shall provide ongoing System Maintenance Services to ensure that all products and Services perform in accordance with this Contract and the applicable SOW. Maintenance Services shall include, at a minimum:

i. Maintaining the System in conformity with the functional and performance requirements set forth in this Contract and the applicable SOW.

ii. Detecting, diagnosing, and correcting System errors, defects, and performance issues consistent with the incident response and resolution described in Section 4.

iii. Performing regular database maintenance and management activities, including backups, optimization, and data integrity assurance, consistent with industry best practices and applicable security standards.
iv. (iv) Performing all Services necessary to maintain a required **99.9 % System Availability** (unless otherwise stated in the applicable SOW), including scheduled preventive maintenance.
v. (v) Participating in periodic meetings with Client Agency (frequency to be defined in each SOW) to review System performance, maintenance activities, Updates, Upgrades, and any planned or unplanned outages.
vi. (vi) Providing Client Agency with electronic access to maintenance and support logs and reports sufficient to monitor status of issues and Contractor Performance.

Each SOW may specify additional or more frequent maintenance deliverables, reporting formats, or communication requirements.

B. Ongoing Support.

1. Contractor shall provide ongoing technical support and system monitoring **24 hours per day, seven days per week, 365 days per year (24 / 7 / 365)** unless otherwise specified in an SOW.
2. Contractor shall monitor all automated or batch processes, as applicable, and initiate immediate escalation and response in the event of any failure or service interruption.
3. Each SOW shall define:

    i. Communication channels (e.g., toll-free support number, email address, or support portal);
    ii. Response time expectations by Severity Level; and
    iii. Escalation procedures and points of contact.

C. Help Desk.

1. Contractor shall maintain a help desk capable of receiving, logging, tracking, and resolving Client Agency technical issues and service requests. At a minimum, the help desk shall:

    i. Provide knowledgeable and trained personnel capable of addressing both functional ("how to") and technical inquiries related to the System.
    ii. Record and track all reported issues, complaints, and service requests in a ticketing or case-management system accessible to Client Agency for review and reporting.
    iii. Maintain and provide a **Frequently Asked Questions (FAQ)** or knowledge-base resource for common issues.
    iv. Respond to Client Agency requests within the applicable response time for the assigned Severity Level, as defined in Section 4.E and the relevant SOW.
    v. Provide Client Agency with periodic help-desk activity reports (at least monthly, unless otherwise specified in the applicable SOW), including summary metrics, unresolved issues, and trend analysis.

2. Each SOW may specify additional requirements, such as on-site dispatch protocols, communication frequency, or detailed reporting formats.

4. **<u>Incident Response and Resolution</u>**

A. Contractor shall promptly respond to and resolve all System issues and service requests (other than Updates, Upgrades, Improvements, or new feature development) in accordance with the Severity Levels defined in the applicable SOW.

B. Each SOW shall specify:

    i. The severity-level definitions and examples of qualifying incidents;
    ii. Target response and resolution timeframes for each Severity Level; and
    iii. Any escalation or notification requirements applicable to critical incidents.

C. If multiple incidents of the same Severity Level are reported concurrently, Client Agency shall determine the order of priority for resolution.

D. The Severity Level of a System issue may be lowered when Contractor implements a work-around, approved by Client Agency, that mitigates the business impact of the issue.

E. Contractor shall use the Severity Levels defined in the table below, which may be refined in each SOW. Each SOW may further refine these definitions and specify response and resolution times appropriate to the covered Services.

SEVERITY LEVEL	DEFINITION	TYPICAL IMPACT
Level 1 – Critical	Complete loss of a core business function or total System outage requiring immediate response.	System unavailable or data integrity compromised.
Level 2 – High	Significant degradation or partial outage with major impact on essential functions.	Key features are inoperative; no immediate workaround.
Level 3 – Medium	Non-critical issue causing limited impact or inconvenience; workaround available.	Minor feature failure or performance issue.
Level 4 – Low	Cosmetic or informational issue not affecting operations.	User interface or documentation error.

5. **System Accuracy**

Contractor shall, at a minimum, conduct an annual performance or accuracy assessment for each deployed system or module, as specified in the applicable SOW. Each SOW shall define the applicable test methodology, data sets, and measurement thresholds for determining System performance and accuracy.

The initial test results will serve as the baseline for ongoing comparison and performance improvement in subsequent assessments.

6. **System Performance, Non-Compliance**

A. If Contractor fails to meet a defined service level during any measurement period, Client Agency shall be entitled to a service credit.

B. The amount of the service credit shall be determined according to the following principles:

i. Tiered Percentage Model: Credits will be applied as a percentage of the monthly service fee for the affected Service. The actual percentages (e.g., 5 %, 10 %, 20 %, 30 %) shall be set forth in each SOW.

ii. Incident-Based Credits: Each SOW may define additional credits for failures to meet response or resolution targets for specific Severity Levels.

iii. Credit Cap: Total service credits in any month shall not exceed 50 % of the Monthly Service Fee for the affected Service.

C. Subject to the applicable SOW, failure to meet any service level metric for three (3) consecutive months or five (5) months in a rolling twelve-month period constitutes **chronic non-performance**, entitling Client Agency to pursue additional remedies available to it under this Contract or otherwise available at law or in equity, including termination for cause.

7. **Minimum Reporting and Transparency Requirements**

Contractor shall provide periodic service level performance reports (at least monthly unless otherwise stated in the applicable SOW) summarizing System Availability, Incidents, and support activity. Contractor shall provide Client Agency with access to data sufficient to independently verify Contractor's reported Performance.

8. **Governance and Review**

Subject to the applicable SOW, the parties shall conduct quarterly service level review meetings to evaluate compliance, performance trends, and potential revisions. Changes to metrics or remedies shall be made only by written amendment executed by both parties.

9. **Order of Precedence**

If an SOW defines specific service levels or credits differing from the requirements set forth in this Exhibit 3, the SOW shall govern for that specific transaction. All other provisions of this Exhibit 3 remain in effect for the remainder of the Term.