

Contract # LS5006

STATE OF UTAH COOPERATIVE CONTRACT

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

Kyndryl Inc		
Name		
1 Vanderbilt Ave		
Address		
New York	NY	10017
City	State	Zip

LEGAL STATUS OF CONTRACTOR

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

K.L 6.17.26

Contact Person Katia Saintfort-Russ Phone #863-581-0468 Email katia.saintfort-russ@kyndryl.com
 Vendor #VC249766 Commodity Code #92005

2. CONTRACT PORTFOLIO NAME: Cloud and Software Solutions
3. PROCUREMENT: This Contract is entered into as a result of Solicitation #BP24-1.
4. CONTRACT PERIOD: Effective Date: 9/16/2026 Termination Date: 9/15/2036 unless terminated early or extended in accordance with the terms and conditions of this Contract. Renewal options (if any): None.
5. Prompt Payment Discount (if any): None. Price Guarantee Period (if any): Minimum Percentage Discount: Life of the contract
 Direct Service Provide Pricing: 1 year
6. ATTACHMENT A: NASPO ValuePoint Master Agreement Terms and Conditions
 ATTACHMENT B: Scope of Work
 ATTACHMENT C: Pricing Catalog
 ATTACHMENT D: Contractor's Response to Solicitation
 ATTACHMENT E: End User Agreements
 ATTACHMENT F: 3rd Party Provider Agreement Template
 ATTACHMENT G: IRS Publication 1075 Exhibit 7
Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.
7. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this Contract.
 - Utah State Procurement Code, Procurement Rules, 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
8. 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 obligations hereunder have been duly authorized and that the Contract is a valid and legal Contract binding on the parties and enforceable in accordance with its terms.
 IN WITNESS WHEREOF, the parties sign and cause this Contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 4 above.

CONTRACTOR

Signed by:

Contractor's Signature

Anita Mikus

Print Name

VP, Kyndryl

Title

6/15/2026

Date

STATE

Signed by:

C38BE9DAC528424...

Director, Division of Purchasing

6/16/2026

Date

ATTACHMENT A

NASPO VALUEPOINT MASTER AGREEMENT TERMS AND CONDITIONS

Negotiated 1.2, 1.13, III.1.3, III.1.4, IV.7, VI.1, VI.1.2, VI.2, V.4.5, VII.5, VII.5.6, IX.1, IX.2, IX.3, IX.3.2, IX.4, IX.5, IX.5.1, IX.5.2, IX.5.3, X.2, X.3, X.5, X.6.1, X.6.2, X.6.3, X.6.4, X.6.5, XI.1, XI.2, XI.3, XII.1, XII.2, XII.2.1, XII.2.1.4, XII.2.2, XII.2.3, XII.2.4, XIII.3, XIII.3.1, XIII.3.3, XIII.3.4, XIII.3.5, XIII.5, XIII.6, XIII.7, XIII.8, XIV.1, XIV.1.1, XIV.2.1, XIV.2.1.1, XIV.2.1.2, XIV.2.1.3, XIV.2.2, XIV.2.2.1, XIV.2.2.2, XIV.2.2.3, XIV.2.2.4, XIV.2.3, XIV.2.4, XIV.2.7, XIV.2.7.1, XIV.3, XIV.3.2, XIV.4, XIV.6, XIV.7, XIV.8.1, XIV.9.1.1, XIV.9.1.3, XIV.9.1.4, XIV.9.2, XIV.9.3, XIV.9.3.2, XIV.9.4, XIV.10, XIV.11, XIV.14

Attachment A1, A 1c, 1d, 3, 3a, 3c, 3f, 4b, 6a, 8c, 9, 9a, 9b, 10, 12, 14a, 15, 17, 18, 23, and 26.

Attachment A1 B 1a, 1d, 1e, 1g, 3, 3a, 3c, 4b, 8c, 9, 9a, 9b, 9c, 10, 12, 14a, 15, 17, 18, 23, 26, 28b, 28c, and 28d.

Attachment A1 C 1d, 1e, 1g, 3, 3a, 3c, 4b, 8a, 8c, 9, 9b, 9c, 10, 12, 14a, 15, 17, 18, 18a, 23 and 26.

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 (1) 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 (2) 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, excluding the information of any customer other than the Participating Entity or Purchasing Entity.

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
Arbitration or Dispute Resolution
- d. Force Majeure
- e. Ordering
- f. Payment (payment schedules and milestones are acceptable)
- g. Termination
- h. Defaults and Remedies
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 Kyndryl Delivery Tools** means software, hardware, and other Kyndryl resources that Kyndryl uses in connection with the Services. Kyndryl has discretion in determining which Kyndryl Delivery Tools it uses. Client may use Kyndryl Delivery Tools only in connection with use of the Services and in accordance with license terms, if any, specified in a SOW. As between Client and Kyndryl, Kyndryl retains ownership of Kyndryl Delivery Tools, including any modifications or enhancements of Kyndryl Delivery Tools made in performance of the Services. Kyndryl Delivery Tools also include Advanced Delivery Tools which are proprietary delivery technologies used to automate the Services.
- 1.14 Lead State** means the State centrally administering any resulting Master Agreement(s) who is a party to this Master Agreement .
- 1.15 Low Risk Data** is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“Low Impact Data”).
- 1.16 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.
- 1.17 Moderate Risk Data** is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“Moderate Impact Data”).
- 1.18 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.
- 1.19 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.
- 1.20 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.
- 1.21 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.).

- 1.22 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.
- 1.23 Participating State** means a state that has executed a Participating Addendum or has indicated an intent to execute a Participating Addendum.
- 1.24 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).
- 1.25 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
- 1.26 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.
- 1.27 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
- 1.28 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.
- 1.29 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, (7) remedies, such as credits, and (8) an explanation of how remedies or credits are calculated and issued.

- 1.30 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
- 1.31 Solicitation** means the Solicitation resulting in this Master Agreement.
- 1.32 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 which may include supplemental or clarifying language in accordance with the terms of this MSA;

III.1.4 The Solicitation, except where a term, requirement, standard, specification, or feature is exceeded by a corresponding term, requirement, standard, specification, or feature in Attachment D: Contractor's response to the Solicitation, in which case the Contractor's response shall take precedence;

III.1.5 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.1.6 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. Unless explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products purchased under this Master Agreement.

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 with 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 Reserved

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 and rates contained in this Master Agreement or offered under this Master Agreement represent the not-to-exceed prices to a Purchasing Entity. Each order will identify the fixed price or, if applicable, the fixed rate (or rates, if variable based on quantity) applicable to the quantity of Product(s) ordered by the Purchasing Entity.

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

VI.1.2 Contractor 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 is normally within thirty (30) days following the date a correct invoice is received. 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 remitted by mail or electronically or may be made via a purchasing card with no additional charge. Purchasing Entity agrees to pay all applicable charges specific for a Product delivered by Contractor including charges for use in excess of authorizations. Charges are exclusive of applicable taxes, levies, tariffs or fees imposed by any governmental authority resulting from Purchasing Entity's acquisitions under this Master Agreement. Charges shall be identified on Contractor's invoice.

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. Contractor may decline an Order if Contractor is unable to meet the Order's requirements.

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 The renewal of an existing service, maintenance, or software subscription may be canceled prior to the renewal 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 Federal, State, and local laws and regulations applicable to Contractor's business.
- 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 an applicable commercial code, if any.
- IX.3 Inspection.** All Products are subject to inspection at reasonable times and places before acceptance. Contractor, if applicable, 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, if applicable, 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 a defect affecting the Product or Service's function, performance, utility, or value 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 applicable industry standards which shall be specified in an Order when applicable, to ascertain whether the Product meets the standard of performance or specifications defined in the associated Order prior to acceptance by the Purchasing Entity.
- IX.5.1** The acceptance testing period will be forty-five (45) calendar days, unless otherwise specified in an Order, 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 will notify Contractor in reasonable detail the requested revisions required by Purchasing Entity so that Product will meet the specification in the Order thereby allowing Contractor to make such requested revisions. If the Purchasing Entity does not provide such detail within the acceptance testing period the Product or Service will be deemed accepted.
- IX.5.3** Contractor will have fifteen (15) calendar days or as otherwise agreed to make such revisions. If after the fifteen (15) calendar day period or as

otherwise agreed, the Product still has not met the standard of performance or specifications defined in the associated Order, the Purchasing Entity may, at its option: (a) declare Contractor to be in breach and terminate the Order; or, (b) provide for an additional time period agreed upon by the Purchasing Entity and the Contractor.

IX.5.4 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 procured by Contractor solely for delivery to and use by Purchasing Entity for a period of 90 days from the date of acceptance, that: (a) the Product performs according to manufacturers' specifications, (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.

X.3 Breach of Warranty. Upon breach of the warranty set forth above, the Contractor will, to the extent allowed by a manufacturer, provide the remedy available from the manufacturer which may include the repair or replacement of the Product whose nonconformance is discovered and made known to the Contractor..

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.

X.6 Disclaimers

X.6.1 Kyndryl does not guarantee that (i) the services will be performed error-free or uninterrupted or that Kyndryl will correct all services errors, (ii) the services will operate in combination with purchasing entity's content or its applications, or with any other hardware or software systems, services, or data not provided by Kyndryl, and (iii) the services will meet purchasing entity's requirements, specifications, or expectations. Purchasing entity acknowledges that Kyndryl does not control the transfer of data over communications facilities, including the internet, and that the services may be subject to limitations, delays, and other problems inherent in the use of such communications facilities.

X.6.2 Kyndryl is not responsible for any delays, delivery failures, or other damage resulting from such problems. Kyndryl is not responsible for any issues related to the performance, operation, or security of the services that arise from purchasing entity's content, its applications, or third-party content that is not provided or sold by Kyndryl. Kyndryl warranties will not apply if there has been misuse, modification, damage not caused by Kyndryl, failure to comply with instructions provided by Kyndryl, or if otherwise stated in an attachment or non- Kyndryl services are sold under the agreement as-is, without warranties of any kind. Third parties may provide their own warranties.

X.6.3 For any breach of services warranty, Purchasing Entity's exclusive remedy and

Kyndryl's entire liability shall be the correction of the deficient services that caused the breach of warranty, or, if Kyndryl cannot substantially correct the deficiency in a commercially reasonable manner, Purchasing Entity may end the deficient services and Kyndryl will refund to Purchasing Entity the fees paid for the deficient services for the period of time during which the Services were deficient.

X.6.4 To the extent not prohibited by law, these warranties are exclusive and there are no other express or implied warranties or conditions including for software, hardware, systems, networks or environments or for merchantability, satisfactory quality and fitness for a particular purpose.

X.6.5 Notwithstanding the foregoing and for the sake of clarity, if Purchasing Entity has a performance concern with the Product, Purchasing Entity will bring such concern directly to Contractor and Contractor in turn will involve the third party as appropriate. Upon such third party's request, Contractor may be required to provide a copy of these terms to such third party, Purchasing Entity authorizes Contractor to comply with such request, and our compliance shall not be deemed a breach of the Confidentiality terms hereunder.

XI. Product Title

XI.1 Project Materials. Unless otherwise set forth in a Participating Addendum or TD, when Contractor provides deliverables as specified in an Order, the Participating Entity will own the copyright in works of authorship that Contractor develops for the Participating Entity as described in a transaction document ("Project Materials"). Project Materials exclude Pre-Existing Intellectual Property.

XI.2 Embedded Software. For Pre-Existing Intellectual Property that are embedded in Project Materials, Contractor grants Participating Entity an irrevocable (subject to Participating Entity's payment obligations), perpetual, nonexclusive, worldwide license to use, execute, reproduce, display, perform and prepare derivatives of . Pre-Existing Intellectual Property that are not Existing License Works, but only to the extent that such Pre-Existing Intellectual Property remains embedded in Project Materials

XI.3 License of Pre-Existing Intellectual Property. Pre-Existing Intellectual Property are works of authorship delivered to the Participating Entity, but not created under the Order, and includes any modifications or enhancements of such Pre-Existing Intellectual Property made during the performance of the Services. Some Pre-Existing Intellectual Property may be subject to a separate license agreement (Existing Licensed Works). A software program is an example of an Existing Licensed Work and is subject to its licensing. For Pre-Existing Intellectual Property that are not embedded in Project Materials and that are not Existing Licensed Works,

Contractor grants to the Purchasing Entity a nonexclusive, , royalty-free, irrevocable (subject to a Purchasing Entity's payment obligations), license to use, reproduce, perform, and display internally, the Pre-Existing Intellectual Property.

XII. Indemnification

XII.1 General Indemnification. General Indemnification. The Contractor shall indemnify and hold harmless by defending (which includes paying fees and related costs of defense) NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers and employees for which they may be legally liable (each, an "Indemnified Party" and collectively, the "Indemnified Parties"), from and against applicable defined third-party claims, damages or causes of action brought against an Indemnified Party for any death, bodily injury, or damage to tangible personal property arising directly from act(s),

error(s), or omission(s) 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 indemnify and hold harmless Purchasing Entities, by defending an Indemnified Party from and against applicable, defined third party claims, damages or causes of action brought against an Indemnified Party, 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 arising from, and Contractor has no responsibility for claims based on, (a) non-Contractor Products or Services; (b) items not provided by Contractor, or (c) any violation of law or third-party rights caused by Client's content, materials, designs, or specifications. The Contractor's obligations under this section shall not extend to any claims arising from, and Contractor has no responsibility for claims based on, the combination of the Product with any other product, system or method, regardless of if 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 or it would be reasonably expected to use the Product in combination with such product, system or method. Contractor has no responsibility for claims based, in whole or part, on Non-Contractor Products, items not provided by Contractor, or any violation of law or third-party rights caused by Participating Entity's content, materials, designs, specifications, or use of a non-current version or release of a Contractor Product when an infringement claim could have been avoided by using a current version or release. Contractor reserves the right to modify or replace a Service with an equivalent non-infringing one or, if replacement is not reasonably available, to discontinue a Service and provide a credit for any pre-paid unexpired term. The Indemnified Parties are responsible for any violation of law or any third-party rights caused by its content or, except as provided in this paragraph, its use of a Service.

This Section XII.2 provides the Indemnified Party's exclusive remedy for any third-party infringement claims or damages.

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. Contractor will defend the Indemnified Party against such claims pursuant to this Section 12, and pay amounts finally awarded by a court against the Indemnified Party or included in a settlement approved by Contractor, provided that the Indemnified Party promptly

(i) notifies Contractor in writing of the claim, (ii) supplies information requested by Contractor as specified in section 12.2.3, and (iii) allows Contractor to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts. 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 held legally liable.

XII.2.3 The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense.

XII.2.4 This section XII is 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 except for Professional Errors and Omissions which is written on a claims made basis. The minimum acceptable limits will be as indicated below:

XIII.3.1 Contractor shall maintain Commercial General Liability insurance covering premises operations, 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:

Level of Risk	Data Breach and Privacy/Cyber Liability including Professional Errors and Omissions 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.3.4 Nothing in this Master Agreement shall be deemed to preclude Kyndryl from selecting a new insurance carrier or carriers or obtaining new or amended policies at any time, as long as the above insurance coverage is maintained. This provision is not intended to, and does not, increase or decrease Kyndryl's liability under the Limitation of Liability provision of this Master Agreement.

XIII.3.5 Professional Errors and Omissions coverage is subject to the following:

- (a) The retroactive date applicable to coverage must precede the effective date of this Contract;
- (b) Continuous coverage shall be maintained for the entire term of this Contract; and
- (c) Such coverages shall remain in place for a period of at least five (5) years beginning from the date that work under this Contract is complete. Proof of such continuing coverage shall be provided to the Purchasing Entity upon request.

- 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 Certificate of Insurance to the Contractor's Commercial 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 Entity as secondary and noncontributory.
- XIII.6 Participating Entities.** Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in Section XIII
- XIII.7 Furnishing of Certificates.** Contractor shall furnish to the Lead State, Participating Entity, and, on request, the copies of certificates of insurance in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. Copies of renewal certificates of all required insurance will be furnished within thirty (30) days after any renewal date to the applicable Lead State or 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 after Contractor's failure to cure (in accordance with section 2.4
- 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 after Contractor's failure to cure (in accordance with section 2.4.

XIV. General Provisions

XIV.1 Records Administration and Audit

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 ("Auditing Entity"), upon thirty (30) days prior written notice, to audit, inspect, examine, take notes with regard to 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 and , notes.

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. Except where contrary to applicable law or otherwise negotiated in a Participating Addendum, any such audit may only occur up to once annually, and the scope of the audit may only cover the three (3) years prior to the date of the audit for each applicable Order. Any Auditing Entity conducting such an audit shall do so during normal business hours with minimal disruption to Contractor's business and agrees that charges or invoices which are included in a previous audit will not be included in a second audit unless otherwise mutually agreed to between the parties. In no event will Service Provider provide its proprietary information or internal costs or external costs during such an audit unless required by applicable law.

XIV.1.1 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 administrative fees found as a result of the examination of the Contractor's records.

XIV.1.2 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. Each party acknowledges that it and its respective 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 the other.

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 the Receiving Party in the performance of this Master Agreement, including but not necessarily limited to (1) any Contractor or Purchasing Entity's records, as applicable (2) personnel records, and (3) information concerning individuals, is confidential information of such party ("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 Receiving Party 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 a party) publicly known; (2) is furnished by Disclosing Party (Purchasing Entity or Contractor) to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Receiving Party's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Contractor or Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of the Disclosing Party (Purchasing

Entity or Contractor as applicable); or (6) is independently developed by employees, agents or Subcontractors of Receiving Party who can be shown to have had not violated this section.

XIV.2.2 Non-Disclosure. Receiving Party shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement or as otherwise allowed under this Master Agreement.

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

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

XIV.2.2.3 Except as directed by Disclosing Party, Receiving Party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Disclosing Party's request, Receiving Party shall turn over to Disclosing Party Receiving Party all documents, papers, and other matter in Receiving Party's possession that embody Confidential Information.

XIV.2.2.4 Notwithstanding the foregoing, Receiving Party 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. Receiving Party acknowledges that Receiving Party's breach of Section 14.2 may cause irreparable injury to the Purchasing Entity that cannot be adequately compensated in monetary damages. Accordingly, Disclosing Party may seek injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Receiving Party acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Disclosing Party and are reasonable in scope and content.

- XIV.2.4 Purchasing Entity Law.** With regard to a Purchasing Entity, 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. Except as allowed under the provisions herein or unless otherwise provided in a contracting document, 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 except for as set forth in this Agreement or applicable law. 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. Assignment of Contractor's rights to receive payments is not restricted. For the avoidance of doubt, the foregoing does not restrict Contractor from assigning, selling, transferring, subcontracting or subletting rights, or delegating responsibilities under a Purchase Order issued against the

Master Agreement if agreed to by the Purchasing Entity.

XIV.3.2 The Lead State may not assign the Master Agreement and no Participating Entity may assign its Participating Addendum, in whole or in part, without the prior approval of Contractor. No Purchasing Entity may give or transfer the Services ordered under an Ordering Document to another individual or entity. Lead State may assign contract administration duties to NASPO ValuePoint and other third parties upon prompt notice to Contractor.

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 consisting of Contract Manager & Report Administrator, managing the Master Agreement. The Lead State reserves the right to approve or reject changes in key personnel, as identified above. 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 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 or the provisions of V.6, 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 material default may be immediate only after being given specific detail of its default and a reasonable period for the opportunity to cure.

XIV.7 Force Majeure. Neither party to this (i) Master Agreement (ii) a Participating Addendum, or (iii) an Ordering Document shall be held responsible for non-monetary delay or default caused by an event, where such occurrence or continuation of such occurrence is beyond the party's reasonable control without fault or negligence on its part and substantially inhibits the party's ability to deliver Product or other deliverables in accordance with this Master Agreement. Such events may include 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. Where the affected party is unable to mitigate the effect of a force majeure event for more than thirty (30) days, the Lead State, Participating Entity, Purchasing Entity, or Contractor, as applicable, may terminate this Master Agreement, the applicable Participating Entity, or the affected Order, as applicable, upon determining such delay or default will reasonably prevent successful performance of the Master Agreement, Participating Addendum, or Order.

XIV.8 Limitation of Liability

XIV.8.1 Except (a) for claims, losses, and liabilities resulting from the recklessness, bad faith, or intentional misconduct of Contractor or its subcontractors, (b) claims, losses, and liabilities arising from death, injury, or damage to tangible property which Contractor has an indemnity obligation hereunder; and (c) each Party's applicable indemnification obligations, each Party's total liability to the other Party related to Services under this Master Agreement, a Participating Addendum, or an Order will be limited to direct damages up to (i) two (2) times the amounts payable under the applicable Order, or (ii) five million dollars (\$5,000,000), whichever is greater. In no event shall Contractor, its affiliates or subcontractors, or their respective personnel be liable to Purchasing Entity for any loss of use, data, goodwill, revenues or profits (whether or not deemed to constitute a direct Claim), or any consequential, special, indirect, incidental, punitive, or exemplary loss, damage, or expense, relating to or in connection with this Master Agreement or any Participating Addendum or Order.

XIV.9 Defaults and Remedies

XIV.9.1 The occurrence of any of the following events will be an event of default under this Master Agreement:

XIV.9.1.1 Nonperformance of material contractual requirements;

XIV.9.1.2 A material breach of any term or condition of this Master Agreement

XIV.9.1.3 Any certification, representation or warranty by Contractor in response to the Solicitation or in this Master Agreement that Contractor knew or should have known to be untrue or materially misleading;

XIV.9.1.4 Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against a party, or the appointment of a receiver or similar officer for a party 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.9.1.5 Any default specified in another section of this Master Agreement.

XIV.9.2 Upon the occurrence of an event of default, the non-breaching party shall issue a written notice of default, identifying the nature of the default, and providing a period of thirty (30) calendar days in which breaching party shall have an opportunity to cure the default. Each party will allow the other party a reasonable opportunity to comply before it claims that the other has not met its obligations under this Master Agreement. The Lead State 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.9.3 If party alleged to be in breach is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, such party shall be in breach of its obligations under this Master Agreement and the non-breaching party shall have

the right to exercise any or all of the following remedies:

XIV.9.3.1 Any remedy provided by law;

XIV.9.3.2 Terminate the applicable portions that are the subject of the material breach in this Master Agreement and any related Contracts or portions thereof;

XIV.9.3.3 Suspension of Contractor's performance; and

XIV.9.3.4 Withholding of payment until the default is remedied.

XIV.9.4 Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, either party 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, either party 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. 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. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under this Master Agreement.

XIV.10 Waiver of Breach. Failure of the Contractor, 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 Contractor, the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Contractor, Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by 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.11 Debarment. To its best knowledge and belief, 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.

XIV.12 No Waiver of Sovereign Immunity

XIV.12.1 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.12.2 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.13 Governing Law and Venue

XIV.13.1 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.13.2 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.13.3 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.14 Assignment of Antitrust Rights. Contractor irrevocably assigns to a Participating Entity who is a state any offensive 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, to the extent that such goods or services were provide to and paid for solely by the Participating Entity.

XIV.15 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 as a Purchasing Entity. 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, 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 Data 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 minimize the possibility of inappropriate or unauthorized use of Public Jurisdiction Data. To this end, the Service Provider shall provide Services designed to safeguard the confidentiality, integrity and availability of Public Jurisdiction Data and comply with the following conditions:

- a. The Service Provider shall implement and maintain appropriate administrative, technical and organizational security measures designed 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 in accordance with the Services requested by the Public Jurisdiction and agreed upon with Service Provider in a SOW.
- b. All Data obtained by the Service Provider in the performance of this contract shall become and remain property of the Public Jurisdiction.
- c. As stipulated in a SOW, 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 Data 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 (except as specified in Section 5 immediately below) 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 Subcontractors 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 Subcontractors to access Public Jurisdiction Data remotely only as required to provide technical support (see also below regarding offshore access and follow the same technical support).

6. Data Access: The Service Provider shall be responsible for:

- a. Providing a multifactor authentication access mechanism for all its personnel and Subcontractors 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 Subcontractors

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 Data 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: Breach Responsibilities: This section only applies when a Data Breach occurs with respect to personal data within Data that has been uploaded into the Services by the applicable Public Jurisdiction.

- a. The Service Provider, unless stipulated otherwise, shall promptly 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 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms 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 within Service Provider's scope of responsibility, if necessary, (3) document actions taken in response to the Data Breach, including any post-incident review of events and changes in business practices, and (4) identifying to the Public Jurisdiction all individuals whose personal information was subject to unauthorized disclosure or access. 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 because Service Provider failed to perform its security obligations and such failure is the cause of the Data Breach causing the unauthorized disclosure or access of personal information, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notify affected individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law for up to twelve (12) months for each affected individual; (4) providing a website or a toll-free number and call center for affected individuals required by state law for up to twelve (12) months; and (5) completing all corrective actions within the Service Provider's scope of responsibility 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 in section XIV.8.

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 Data. 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 dedicated 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 a, the Service Provider shall promptly 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 available 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 infrastructure designed to be secure (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 or as otherwise agreed upon. 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 (provided such contractor is not a competitor of Service Provider) 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. In no event will Service Provider provide its proprietary information or internal costs or external costs during such an audit unless required by applicable law.

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 mandated regulatory government agency's information security office access to view the audit and artifacts through StateRAMP, if applicable where the certifications provided for such data center and any clarifying information regarding such artifacts are insufficient for the mandated regulatory agency. Some governments may accept a multi customer SOC 2 Type 2 audit annually, if available, 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 summary of its business continuity plan upon request and disaster recovery plan where agreed upon in a SOW and ensure that the recovery time objective (RTO) identified by the Public Jurisdiction in an SOW 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 Service Provider'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 as a Purchasing Entity. 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, 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 notifications
- g. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal Data or non-public Data the Service Provider believes has a significant probability of resulting 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 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 minimize the possibility of inappropriate or unauthorized use of Public Jurisdiction Data at any time. To this end, the Service Provider shall provide Services designed to safeguard the confidentiality, integrity and availability of Public Jurisdiction Data and comply with the following conditions:

- a. The Service Provider shall implement and maintain appropriate administrative, technical and organizational security measures designed 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 in accordance with the Services requested by the Public Jurisdiction and agreed upon with Service Provider in a SOW or an Order.
- b. All Data obtained by the Service Provider in the performance of this contract shall become and remain property of the Public Jurisdiction.
- c. As stipulated in a SOW, 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.

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 (except as specified in Section 5 immediately below) 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 Subcontractors 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 Subcontractors 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 Subcontractors 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 offshore access by Service Provider employees and Subcontractors unless explicitly authorized by the Purchasing Entity for follow the sun technical support.

- b. 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 Data 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 Data that has been uploaded into the Services by the applicable Public Jurisdiction.

- a. The Service Provider, unless stipulated otherwise, shall promptly 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 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms 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 within Service Provider's scope of responsibility, 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, and (4) identifying to the Public Jurisdiction all individuals whose personal information was subject to unauthorized disclosure or access.
- 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 because Service Provider failed to perform its security obligations and such failure is the cause of the Data Breach causing the unauthorized disclosure or access of personal information, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifying affected individuals, regulators or others required by

state law; (3) providing a credit monitoring service required by state or federal law for up to twelve (12) months for each affected individual; (4) providing a website or a toll-free number and call center for affected individuals required by state law for up to twelve (12) months; and (5) completing all corrective actions within the Service Provider's scope of responsibility 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 in section XIV.8.

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 Data. 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 dedicated 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 and if Service Provider agrees, the Service Provider shall promptly 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 available 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 infrastructure designed to be secure (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 or as otherwise agreed upon. 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 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 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 financial audit of conformance to the contract terms. The Public Jurisdiction or a contractor of its choice (provided such contractor is not a competitor of Service Provider) 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. In no event will Service Provider provide its internal or external costs during such an audit unless required by applicable law.

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 mandated regulatory government agency's information security office access to view the audit and artifacts through StateRAMP, if applicable where the certifications provided for such data center and any clarifying information regarding such artifacts are insufficient for the mandated regulatory agency. Some governments may accept a multi customer SOC 2 Type 2 audit annually, if available, 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 summary of its business continuity plan upon request and disaster recovery plan upon where agreed upon in a SOW and ensure that the Public Jurisdiction's recovery time objective (RTO) identified by the Public Jurisdiction in an SOW 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 Service Provider'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 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 Data.
- d. After termination of the contract and the prescribed retention period, the Service Provider shall securely dispose of all digital content in all forms, such as disk, CD/

DVD, backup tape and paper. The Public Jurisdiction's 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 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. **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 as a Purchasing Entity. 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, 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 notifications.
- g. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal Data or non-public Data the Contactor believes could reasonably result with significant probability 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 s 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 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 minimize the possibility inappropriate or unauthorized use of Public Jurisdiction Data at any time. To this end, the Service Provider shall provide Services designed to safeguard the confidentiality, integrity and availability of Public Jurisdiction Data and comply with the following conditions:

- a. The Service Provider shall implement and maintain appropriate administrative, technical and organizational security measures designed 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 in accordance with the Services requested by the Public Jurisdiction and agreed upon with Service Provider in a SOW.
- b. All Data obtained by the Service Provider in the performance of this contract shall become and remain property of the Public Jurisdiction.
- c. As stipulated in a SOW, 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. 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.

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 (except as specified in Section 5 immediately below) 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 Subcontractors 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 Subcontractors 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 Subcontractors 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 Subcontractors 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 Data 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 and take 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 Data that has been uploaded into the Services by the applicable Public Jurisdiction.

- a. The Service Provider, unless stipulated otherwise, shall promptly 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 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms 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 within Service Provider's scope of responsibility, 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, and (4) identifying to the Public Jurisdiction all individuals whose personal information was subject to unauthorized disclosure or access.
- 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 because Service Provider failed to perform its security obligations and such failure is the cause of the Data Breach causing the unauthorized disclosure or access

of personal information, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifying affected individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law for up to twelve (12) months for each affected individual; (4) providing a website or a toll-free number and call center for affected individuals required by state law for up to twelve (12) months; and (5) completing all corrective actions within the Service Provider's scope of responsibility 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 in section XIV.8.

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 Data. 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 dedicated 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 and if the Service Provider agrees, the Service Provider shall promptly 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 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 available 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 or as otherwise agreed upon. 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: Not relevant to service model. Standards would be selected by the Public Jurisdiction.

17. Contract Audit: The Service Provider shall cooperate with Public Jurisdiction financial audit of conformance to the contract terms. The Public Jurisdiction or a contractor of its choice (provided such contractor is not a competitor of Service Provider) 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. In no event will Service Provider provide its internal or external costs during such an audit unless required by applicable law.

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 mandated regulatory government agency's information security office access to view the audit and artifacts through StateRAMP, if applicable where the certifications provided for such data center and any clarifying information regarding such artifacts are insufficient for the mandated regulatory agency.

- a. Some governments may accept a multi customer SOC 2 Type 2 audit annually, if available, 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
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 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 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 summary of its business continuity plan upon request and disaster recovery plan upon where agreed upon in a SOW and ensure that the Public Jurisdiction's recovery time objective (RTO) identified by the Public Jurisdiction in an SOW 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 Service Provider'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 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 Data.
- d. After termination of the contract and the prescribed retention period, 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 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. Fulfillment 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 data¹ 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. Fulfillment 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)	5%	5%	5%	5%	5%
Value-Added Resellers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	5%	5%	5%	5%	5%
Maximum Markup %	Software (Saas)	Infrastructure (Iaas)	Platform (Paas)	On-Premises	Value Added Services*
Value-Added Resellers: Maximum Markup %	50%	50%	50%	50%	50%

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:

Attachment G
IRS Publication 1075 Exhibit 7

Exhibit 7 Safeguarding Contract Language

I. PERFORMANCE

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

- (1) All work will be performed under the supervision of the contractor.
- (2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- (3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- (4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- (5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- (7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- (8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- (9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- (10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.
- (11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and

obligated to the agency under this contract.

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

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

II. CRIMINAL/CIVIL SANCTIONS

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

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

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

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

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

III. INSPECTION

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