

**Participating Addendum for
Cloud and Software Solutions
between
State of Iowa – 2027-BUS-8007
and
DLT Solutions LLC**

This Participating Addendum is entered into by the State of Iowa – Department of Management (“Participating Entity”) and the following Contractor (each a “Party” and collectively the “Parties”) for the purpose of participating in NASPO ValuePoint Master Agreement Number LS4992, executed by Contractor and Utah (“Lead State”) for Cloud and Software Solutions (“Master Agreement”):

DLT Solutions LLC (“Contractor”)
2411 Dulles Corner Park
Herndon, VA 20171

I. PARTICIPATING ADDENDUM CONTACTS.

Contractor's contact for this Participating Addendum is:

Adam Pritchard
ProgramManagement@dlt.com
703-773-8988

Participating Entity's contact for this Participating Addendum is:

IT Contracts
ITContracts@dom.iowa.gov
515-672-4569

- II. TERM.** This Participating Addendum is effective as of the date of the last signature below or **September 16, 2026**, whichever is later, and will terminate upon termination of the Master Agreement on **September 15, 2036**, unless the Participating Addendum is terminated sooner in accordance with the terms set forth herein.
- III. PARTICIPATION AND USAGE.** This Participating Addendum may be used by all state agencies, institutions of higher education, cities, counties, districts, and other political subdivisions of the state, and nonprofit organizations within the state if authorized herein and by law. Participating Entity has sole authority to determine which entities are eligible to use this Participating Addendum. If Contractor becomes aware that an entity's use of this Participating Addendum is not authorized, Contractor will notify NASPO ValuePoint to initiate outreach to the appropriate parties.
- IV. GOVERNING LAW.** The construction and effect of this Participating Addendum and any Orders placed hereunder will be governed by, and construed in accordance with, Participating Entity's laws.
- V. SCOPE.** Except as otherwise stated herein, this Participating Addendum incorporates the scope, pricing, terms, and conditions of the Master Agreement and the rights and obligations set forth therein as applied to Contractor and Participating Entity and Purchasing Entities.
- a. Products.** All products available through the Master Agreement may be offered and sold by Contractor to Purchasing Entities.
 - b. Services.** All services available through the Master Agreement may be offered and sold by Contractor to Purchasing Entities.
 - c. Contractor Partners.** All subcontractors, dealers, distributors, resellers, and other partners identified on Contractor's NASPO ValuePoint webpage as authorized to provide Products and Services to Participating Entity may provide Products and Services to users of this Participating Addendum. Contractor will ensure that the participation of Contractor's subcontractors, dealers, distributors, resellers, and other partners is in accordance with the terms and conditions set forth in the Master Agreement and in this Participating Addendum.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- d. Any amendment to the Master Agreement shall be deemed incorporated into this Participating Addendum unless the amendment is rejected by Participating Entity in writing to Contractor within ten (10) calendar days of the amendment's effective date and is documented thereafter via written amendment hereto.
- e. **Any conflict between this Participating Addendum and the Master Agreement will be resolved in favor of the Participating Addendum.** The terms of this Participating Addendum, including those modifying or adding to the terms of the Master Agreement, apply only to the Parties and shall have no effect on Contractor's participating addenda with other participating entities or Contractor's Master Agreement with the Lead State.

VI. ORDERS. Purchasing Entities may place orders under this Participating Addendum by referencing the Participating Addendum Number on an Order. Each Order placed under this Participating Addendum is subject to the pricing and terms set forth herein and in the Master Agreement, including applicable discounts, reporting requirements, and payment of administrative fees to NASPO ValuePoint and Participating Entity, if applicable.

VII. FEDERAL FUNDING REQUIREMENTS. 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. When applicable, a Purchasing Entity will identify in the Order any alternative or additional requirements related to the use of federal funds. By accepting the Order, Contractor agrees to comply with the requirements set forth therein.

VIII. ORDER OF PRECEDENCE – DOCUMENTS INCORPORATED

Nonnegotiable Statutory Terms. Certain terms of this Agreement are nonnegotiable and apply to every entity that procures using this vehicle. Terms prohibited by Iowa Code section 8.94 are void, the terms required by Iowa Code section 8.95 are included, and any limitation of Vendor liability is subject to Iowa Code section 8.96. See Attachment A, Section 1.1.

This Agreement and all attachments and external documents identified below are incorporated by this reference and together comprise the terms and conditions governing the relationship between the Parties, to be interpreted in the following order of precedence:

Notwithstanding the order set forth below, the Nonnegotiable Statutory Terms in Attachment A, Section 1.1 control over every document and term listed below.

- a. Ancillary agreements unique to a Purchasing Entity making purchases hereunder that specifically address state, local, or federal regulatory or compliance concerns and which may be incorporated via a Purchasing Instrument;
 - b. The following documents are incorporated by reference solely to establish their potential applicability and order of precedence. These documents shall apply to the extent expressly designated as applicable in a Purchasing Instrument executed hereunder. Inclusion of a reference in this section shall not, in itself, impose an obligation on Vendor unless and until such obligation is expressly incorporated into a Purchasing Instrument.
 - i. The IT Business Associate Agreement ("BAA"), which may be updated from time to time to conform with applicable federal laws, a current version of which is available at: <https://dom.iowa.gov/media/222>;
 - ii. The IRS Publication 1075 Exhibit 7, which may be updated from time to time to conform with applicable laws, a current version of which is available at: [Publication 1075 \(Rev. 11-2021\)](#);
 - iii. The Federal Certifications, which may be updated from time to time to conform to applicable federal law, a current version of which is available at

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

<https://dom.iowa.gov/media/377>;

- iv. Iowa Code chapter 8F.
- c. The terms of any Purchasing Instruments executed hereunder;
- d. General Terms and Conditions (Attachments A and B);
- e. The Underlying Agreement;
- f. The Solicitation;
- g. The Proposal.

IX. ATTACHMENTS. This Participating Addendum includes the following attachments:

- a. Attachment A: Participating Entity Modifications and Additions to Master Agreement Terms and Conditions
- b. Attachment B: Participating Entity Data Protection Addendum

X. NOTICE. Any notice required herein shall be sent to the following:

For Contractor:

Adam Pritchard
adam.pritchard@dlt.com
703-773-8988

For Participating Entity:

Department of Management
Office of the General Counsel
domlegalnotices@iowa.gov

XI. SUBMISSION OF PARTICIPATING ADDENDUM TO NASPO VALUEPOINT. Upon execution, Contractor shall promptly email a copy of this Participating Addendum and any amendments hereto to NASPO ValuePoint at pa@naspovaluepoint.org. The Parties acknowledge and agree that the Participating Addendum, as amended, may be published on the NASPO ValuePoint website.

SIGNATURE

The undersigned for each Party represents and warrants that this Participating Addendum is a valid and legal agreement binding on the Party and enforceable in accordance with the Participating Addendum's terms and that the undersigned is duly authorized and has legal capacity to execute and deliver this Participating Addendum and bind the Party hereto.

IN WITNESS WHEREOF, the Parties have executed this Participating Addendum.

CONTRACTOR:

Steve Wells

Signature

Steve Wells

Printed Name

Vice President, PMO & Operations

Title

8/5/2026

Date

PARTICIPATING ENTITY:

Kraig Paulsen

Signature

Kraig Paulsen

Printed Name

Director, Dept of Mgmt

Title

8/14/2026 | 9:03 AM CDT

Date

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

Attachment A

General Terms and Conditions

The parties may be referred to herein individually as a **“Party”** or collectively as the **“Parties.”** The Parties agree to the following:

1. Overview.

- 1.1. Nonnegotiable Statutory Terms. The following terms are nonnegotiable. Because this Agreement is entered into by DOM pursuant to subchapter XI of Iowa Code chapter 8, the terms prohibited by Iowa Code section 8.94 are void, and the terms required by Iowa Code section 8.95 are included in this Agreement by operation of law. These terms apply to every Purchasing Instrument executed under this Agreement and thereby flow down to and apply for the benefit of each Purchasing Entity. This subsection controls over any conflicting term in this Agreement, a Purchasing Instrument, the Underlying Agreement, the Solicitation, the Proposal, or any Additional Terms.
 - 1.1.1. Prohibited terms are void. Any term prohibited by Iowa Code section 8.94 is void and unenforceable, and this Agreement and each Purchasing Instrument shall be interpreted and enforced as if the term were not included, wherever the term appears.
 - 1.1.2. Required terms are included. The terms required by Iowa Code section 8.95, including its State data provision, are deemed included. Where a section 8.95 term grants the State or a Purchasing Entity greater rights than this Agreement otherwise provides, the section 8.95 term controls; where this Agreement grants greater rights, this Agreement controls.
 - 1.1.3. Limitation of Vendor liability. Any limitation of Vendor liability, wherever it appears, is subject to Iowa Code section 8.96 and is void to the extent it repudiates liability for a cybersecurity incident; limits liability for intentional torts, criminal acts, fraud, intentional or willful misconduct, gross negligence, death, bodily injury, damage to real or personal property, intellectual property violations, liquidated damages, compliance with applicable law, violation of confidential information obligations, or Vendor’s indemnification obligations; does not apply equally to the Parties; or limits Vendor liability to less than the contract value inclusive of all extensions.
 - 1.1.4. Contract terms not confidential. Nothing in this Agreement, a Purchasing Instrument, or any Additional Terms renders the terms of this Agreement or any pricing or payment information confidential.
- 1.2. Relationship between this Agreement and Individual Purchasing Instruments. Each Purchasing Instrument executed hereunder shall be deemed, upon its execution, to incorporate the terms and conditions of this Agreement and shall constitute a separate, distinct, and independent Agreement between Vendor and the applicable Purchasing Entity. To the extent a Purchasing Entity other than DOM makes a purchase hereunder pursuant to a Purchasing Instrument executed by it, such Purchasing Entity shall be solely responsible for any payments due, duties, and obligations otherwise owed Vendor under the separate Purchasing Instrument. In addition, notwithstanding any other provision of this Agreement to the contrary, DOM bears no obligation or liability for any other

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

Purchasing Entity's losses, liabilities, or obligations, including Vendor's failure to perform, arising out of or relating in any way to this Agreement. Likewise, the State of Iowa generally bears no obligation or liability for any political subdivision or other non-State Entity's losses, liabilities, or obligations, including the Vendor's failure to perform, arising out of or relating in any way to this Agreement.

1.3. **Incorporation of the Underlying Agreement.**

1.3.1. Governmental entities making purchases hereunder shall be afforded all of the rights, privileges, warranties, and indemnifications afforded by the Underlying Agreement, and such rights, privileges, warranties, and indemnifications shall accrue and apply with equal effect to governmental entities making purchases hereunder. Except as otherwise provided herein or in a Purchasing Instrument, Vendor shall perform all duties, responsibilities, and obligations required under the Underlying Agreement in the time and manner specified thereunder. In the event of any conflict or inconsistency between the terms and conditions of this Agreement and the Underlying Agreement, such conflict or inconsistency shall be resolved as stated on the CD&E.

1.3.2. Any references in the Underlying Agreement to the governmental entity or its governmental units, or to rights and privileges granted to such governmental units, shall be interpreted to mean the State of Iowa and its equivalent governmental entities for the purposes of this Agreement. Similarly, any references to the governmental entity statutes, regulations, case law, or other legal authorities shall be construed as references to the corresponding Iowa legal authorities addressing substantially similar subject matter.

2. **Definitions.** In addition to any other terms that may be defined elsewhere in this Agreement, the following terms shall have the following meanings:

2.1. **"Acceptance"** means the Purchasing Entity has determined a portion of the Deliverables satisfies its Acceptance Tests. **"Final Acceptance"** means the Purchasing Entity has determined all Deliverables satisfy the Purchasing Entity's Acceptance Tests. **"Non-acceptance"** means the Purchasing Entity has determined that a portion of or all of the Deliverables have not satisfied the Purchasing Entity's Acceptance Tests.

2.2. **"Acceptance Criteria"** means the Specifications, goals, performance measures or standards, testing results, requirements, technical standards, representations, or other criteria designated by the Purchasing Entity and against which Acceptance Tests are conducted, including any of the foregoing stated or expressed in this Agreement, a Purchasing Instrument, the Solicitation, the Proposal, any Documentation, and any applicable state, federal, foreign, and local laws, rules, and regulations.

2.3. **"Acceptance Tests" or "Acceptance Testing"** means the tests, reviews, and other activities that are performed by or on behalf of the Purchasing Entity to determine whether any or all Deliverables meet Acceptance Criteria or otherwise satisfy the Purchasing Entity, as determined by the Purchasing Entity in its sole discretion.

2.4. **"AI" or "Artificial Intelligence"** means a machine-based system that is designed to autonomously or semi-autonomously generate or materially modify content, code, recommendations, or decisions that can influence physical or virtual environments. For purposes of this Agreement, AI does not include incidental or embedded software features whose primary purpose is to assist with routine

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- tasks (such as spell-check, grammar suggestions, or basic data sorting) and which do not independently generate or materially modify Deliverables under this Agreement.
- 2.5. **“Authorized Contractors”** means independent contractors, consultants, or other third parties that are retained, hired, or utilized by the Purchasing Entity in any way to assist the Purchasing Entity with any Deliverables provided hereunder.
- 2.6. **“Confidential Information”** means, subject to any applicable federal, state, or local laws and regulations, including Iowa Code Chapter 22, any confidential or proprietary information or trade secrets disclosed by either Party (**“Disclosing Party”**) to the other Party (**“Receiving Party”**) that, at the time of disclosure, is designated as confidential (or like designation), is disclosed in circumstances of confidence, or would be understood by the Parties, exercising reasonable business judgment, to be confidential. Confidential Information does not include any information that: (i) was previously and rightfully in the possession of the Receiving Party from a source other than the Disclosing Party; (ii) was known to the Receiving Party prior to the disclosure of the information by the Disclosing Party; (iii) was disclosed to the Receiving Party without restriction by an independent third party having a legal right to disclose the information; (iv) is in the public domain; (v) is independently developed by the Receiving Party without any reliance on Confidential Information disclosed by the Disclosing Party; (vi) is disclosed or is required or authorized to be disclosed in compliance with applicable law; or (vii) is disclosed by the Receiving Party with the written consent of the Disclosing Party.
- 2.7. **“Customer Data”** means all information, data (including de-identified and aggregated data), materials, or documents (including Confidential Information and Personal Data) originating with, disclosed by, provided by, made accessible by, or otherwise obtained by or from the Purchasing Entity, the State of Iowa, or users, directly or indirectly, including from any Authorized Contractors of any of the foregoing, related to this Agreement in any way whatsoever, regardless of form, including all information, data, materials, or documents accessed, used, or developed by Vendor in connection with any Customer-Owned Deliverables provided hereunder and all originals and copies of any of the foregoing.
- 2.8. **“Customer Property”** means any property, whether tangible or intangible, of or belonging to the Purchasing Entity, including Customer Data and Customer-Owned Deliverables, software, hardware, programs, or other property possessed, owned, or otherwise controlled, maintained, or licensed by the Purchasing Entity, including third party software or Third-Party Intellectual Property.
- 2.9. **“Customer-Owned Deliverables”** means any Deliverables specifically created or developed by Vendor at the direction of the Purchasing Entity pursuant to a Purchasing Instrument, including all associated intellectual property rights, such as copyrights, patents, trade secrets, trademarks, Source Code, and related Documentation, but excluding Vendor Materials.
- 2.10. **“Deficiency”** means a defect, flaw, error, bug, failure, omission, interruption of service, or other problem of any nature whatsoever related to a Deliverable(s), including any failure of a Deliverable(s) to conform to or meet an applicable Specification. Deficiency also includes the lack of something essential or necessary for completeness or proper functioning of a Deliverable(s).
- 2.11. **“Deliverables”** means all of the services, goods, software, work, work product, items, materials, and property to be created, developed, produced, delivered, performed, or provided by or on behalf of,

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

or otherwise made available through, Vendor, directly or indirectly, in connection with this Agreement.

- 2.12. **“Documentation”** means any and all technical information, commentary, explanations, design documents, system architecture documents, database layouts, code, test materials, training materials, guides, manuals, worksheets, notes, work papers, and all other information, documentation, and materials discovered, created, or developed by Vendor hereunder or otherwise related to or used in conjunction with any Deliverables in any medium, including hard copy, electronic, digital, and magnetically, or optically encoded media.
- 2.13. **“DOM”** means the State of Iowa Department of Management and, unless the context clearly indicates otherwise, any independent contractors, consultants, or other third parties (including other governmental entities) who are retained, hired, or utilized by DOM in furtherance of this Agreement.
- 2.14. **“Personal Data”** means any information relating to an identified or identifiable person, including, but not limited to, Social Security or other government-issued identification numbers, federal or state tax information, “Personal Information” as defined in Iowa Code 715C, account security information, financial account information, credit/debit/gift or other payment card information, account passwords, intellectual property, document identification number, and sensitive or personal data (or equivalent terminology) as defined under any applicable law regarding privacy, data protection, information security obligations, or the Processing of Personal Data.
- 2.15. **“Process”** or **“Processing”** shall mean any operation or set of operations performed upon the Personal Data, whether or not by automatic means, including collection, recording, organization, use, transfer, disclosure, storage, manipulation, combination, and deletion of Personal Data.
- 2.16. **“Proposal”** means the Vendor’s response to the Solicitation.
- 2.17. **“Purchasing Entity”** means the governmental entity that signs a Purchasing Instrument and, unless the context clearly indicates otherwise, any independent contractors, consultants, or other third parties who are retained, hired, or utilized by the Purchasing Entity in furtherance of the Purchasing Instrument or this Agreement.
- 2.18. **“Purchasing Instrument”** means an individual transactional document executed hereunder for the purchase of Deliverable(s) pursuant to this Agreement, regardless of form, and which identifies the specific Deliverable(s) to be purchased and any Acceptance Criteria or Specifications related thereto.
- 2.19. **“Source Code”** means the human-readable source code, source program, scripts, in any language or form, for or related to any software. Source Code includes all source code listings, instructions (including compile instructions), programmer’s notes, commentary, and all related technical information and Documentation, including all such information and Documentation that is necessary or useful for purposes of maintaining, repairing, or making modifications, or updates, upgrades, bug fixes, patches, or additions to the Deliverable.
- 2.20. **“Specifications”** means any and all requirements, technical standards, performance standards, representations, warranties, and other criteria related to any Deliverables, described or stated in this Agreement (including any exhibit or Documentation attached to, or provided in connection with, this Agreement), any Purchasing Instrument(s), the Solicitation, the Proposal, and, solely to the extent not inconsistent with the foregoing, the Documentation.

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 2.21. **“Third Party Intellectual Property”** shall mean intellectual property, including third-party software, licensed, made, conceived, or developed by a third party and provided or used by or on behalf of the Purchasing Entity or Vendor.
- 2.22. **“Vendor”** means the entity identified on the CD&E including any employees, agents, independent contractors, or any other staff or personnel acting on behalf of or at the direction of Vendor, which personnel may alternatively be referred to as **“Vendor Personnel”**, and which includes any Vendor contractor performing or providing services or Deliverables under this Agreement.
- 2.23. **“Vendor Materials”** means all pre-existing materials, including software, methodologies, tools, techniques, processes, and know-how owned by Vendor.

3. Services and Deliverables.

- 3.1. *Generally.* The Vendor will perform all work and provide all Deliverables in accordance with this Agreement, as well as any associated Purchasing Instrument.
- 3.2. *Purchasing Instruments.*
 - 3.2.1. *Generally.* The Parties may execute individual Purchasing Instrument(s) identifying specific Deliverables to be provided hereunder. Once a Purchasing Instrument has been executed, the Vendor will carry out and complete the duties and responsibilities set forth in the applicable Purchasing Instrument in accordance with the terms of this Agreement as well as any additional or substitute terms provided in the specific Purchasing Instrument.
 - 3.2.2. *Effect of Purchasing Instruments.* A Purchasing Entity executing a Purchasing Instrument pursuant to this Agreement may agree to additional terms and conditions in a Purchasing Instrument that are in conflict with or inconsistent with the terms and conditions of this Agreement. Such Purchasing Instrument terms apply only to the scope of work identified in the Purchasing Instrument and do not alter the agreed terms in this Agreement. Notwithstanding the foregoing, the following terms of this Agreement shall always control regardless of any contrary terms that may be in a Purchasing Instrument:
 - 3.2.2.1. The Nonnegotiable Statutory Terms in Section 1.1;
 - 3.2.2.2. Information contained on the CD&E;
 - 3.2.2.3. The definition of Confidential Information;
 - 3.2.2.4. Set-off obligations under section 4.8;
 - 3.2.2.5. Compliance with the Law under section 7.7;
 - 3.2.2.6. No Conflicts obligations under section 7.8;
 - 3.2.2.7. Termination provisions in section 9;
 - 3.2.2.8. The General Provisions set forth in Section 11.
- 3.3. *Delivery.*
 - 3.3.1. *Risk of Loss.* To the extent any Deliverable(s), including any hardware or equipment, are mailed or shipped, Vendor shall bear all freight, shipping, handling, and insurance costs for the delivery and shall bear all risk of loss that may occur prior to the Purchasing Entity’s Acceptance.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 3.3.2. *Documentation.* Vendor will, at no charge to the Purchasing Entity, provide to the Purchasing Entity all Documentation related to the Deliverable(s) unless otherwise agreed to by the Purchasing Entity in writing.
- 3.3.3. *Source Code Release and License Rights.* Vendor shall, upon the occurrence of any of the triggering events described in this Section, provide the State with a complete, accurate, and up-to-date copy of the source code and related documentation for all software and systems provided under this Agreement (“Source Code”), including any third-party components to the extent the Vendor has rights and authority to provide such components to the State. This obligation applies to all software and components used to deliver the solution licensed or provided to the State under this Agreement.
 - 3.3.3.1. *Triggering Events.* The State shall be entitled to immediate delivery of the Source Code upon the occurrence of any of the following events (each, a “Triggering Event”):
 - 3.3.3.1.1. Vendor becomes insolvent, files for bankruptcy protection, is placed into receivership, or otherwise ceases doing business in the ordinary course;
 - 3.3.3.1.2. Vendor materially abandons or ceases to support or maintain the software in a manner that prevents the State from continuing its normal business operations using the software;
 - 3.3.3.1.3. Vendor voluntarily ceases the provision of services under this Agreement and fails to provide sufficient transition assistance or alternatives to prevent disruption to the State’s critical business functions.
 - 3.3.3.2. *Rights Upon Release.* Upon the occurrence of a Triggering Event and delivery of the Source Code, the State shall have a non-exclusive, perpetual, irrevocable, fully paid-up, royalty-free, worldwide license to use, modify, and create derivative works of the Source Code solely for purposes of operating, maintaining, and supporting the State’s internal business processes. The State shall not disclose the Source Code to any third party except to the extent necessary for such operation and support and subject to written confidentiality obligations no less protective than those in this Agreement.
 - 3.3.3.3. *Delivery.* Within ten (10) business days following a written request by the State upon the occurrence of a Triggering Event, Vendor shall deliver the Source Code and all associated documentation, build instructions, configuration files, and dependencies in a format that is complete, functional, and sufficient to allow a reasonably skilled software developer to maintain and operate the software.

4. Compensation and Additional Rights and Remedies.

- 4.1. Pricing/Compensation. The fees for the services and/or Deliverables provided by the Vendor shall be in accordance with the obligations of this Agreement and the applicable Purchasing Instrument.
- 4.2. No Additional Fees. Other than as permitted by Section 4.1 (Pricing/Compensation) or by Purchasing Instrument, the Purchasing Entity shall not be obligated to pay any other amounts to the Vendor, specifically including travel, lodging, and related expenses. In no event shall the Purchasing Entity be

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

responsible for payment of Vendor's performance costs incurred in connection with this Agreement, including but not limited to equipment, supplies, personnel, salaries, benefits, insurance, training, conferences, telephone, utilities, start-up costs, and all other operational and administrative costs and expenses. To the extent any Purchasing Instrument calls for reimbursement of travel, such travel charges may never exceed the amounts allowed under DAS-SAE travel policy, DAS-SAE Title 210. (available at: <https://das.iowa.gov/state-employees/travel-and-relocation/210-travel>). For vendors, travel reimbursement may not exceed the amounts that would be payable under DAS-SAE 210.245. (available at: https://das.iowa.gov/sites/default/files/acct_sae/sae_manual/210/210-245.pdf). In addition, in-state lodging reimbursement is limited to providers certified by the Iowa Department of Public Safety's Human Trafficking Prevention Training.

- 4.3. Satisfactory Performance. Vendor is not entitled to payment for any services or Deliverable(s), in whole or in part, provided under this Agreement or any Purchasing Instrument(s) if the Purchasing Entity reasonably determines that such services or Deliverable(s) have not been satisfactorily or completely delivered or performed.
- 4.4. Payment does not Imply Acceptance. Payment, including final payment, shall not be construed as acceptance of any services or Deliverables with Deficiencies or incomplete work, and Vendor shall remain responsible for compliance with its contractual obligations. Vendor's acceptance of the last payment from the Purchasing Entity shall operate as a release of any and all claims related to this Agreement concerning the Purchasing Entity's obligations under this Agreement.
- 4.5. Invoices. Upon receipt of written notice of Acceptance from the Purchasing Entity Vendor shall submit an invoice to the Purchasing Entity requesting payment of the fees or other compensation to which it is entitled pursuant to the applicable Purchasing Instrument, less any agreed upon Retained Amount(s) or other applicable offsets. The Purchasing Entity will verify Vendor's performance/provisioning of services or Deliverable(s) outlined in the invoice before making payment. The Purchasing Entity shall pay all approved invoices in arrears and, to the extent applicable, in conformance with Iowa Code section 8A.514 and corresponding implementing rules, regulations, and policies. The Purchasing Entity may pay in less than 60 days, but an election to pay in less than 60 days shall not, to the extent applicable, act as an implied waiver of Iowa Code section 8A.514. Notwithstanding anything herein to the contrary, the Purchasing Entity shall have the right to dispute any invoice submitted for payment and withhold payment of any disputed amount if the Purchasing Entity believes the invoice is inaccurate or incorrect in any way. Vendor shall submit all invoices for payment to the Purchasing Entity, by August 1 for all services performed in the preceding state fiscal year (the State fiscal year ends June 30). If the Vendor seeks payment for end of state fiscal year claims submitted after August 1, the Vendor may submit the late claims, but the Purchasing Entity will only reimburse the claims if funding is available and the Purchasing Entity is legally authorized to make payment. If funding is not available after the end of the state fiscal year, the Vendor may submit the claim to the Iowa State Appeal Board for a final decision regarding reimbursement of the claim.
- 4.6. Retention. To secure Vendor's performance under this Agreement, a Purchasing Entity may retain a mutually agreed upon percentage of the fees or other compensation associated with each Deliverable provided under a Purchasing Instrument ("**Retained Amounts**") until all Deliverables under such Purchasing Instrument have been provided and the Purchasing Entity has given its Final Acceptance. Retained Amounts shall be payable upon the Purchasing Entity's delivery of written notice of Final Acceptance, subject to the terms and conditions hereof.

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 4.7. Erroneous Payments and Credits. The Vendor shall promptly pay or refund to the Purchasing Entity the full amount of any overpayment or erroneous payment within ten (10) business days after either discovery by the Vendor or notification by the Purchasing Entity of the overpayment or erroneous payment. If the Vendor fails to provide a timely refund pursuant to this obligation, a simple interest of one percent (1%) per month may be charged on the outstanding balance unless one percent (1%) exceeds the maximum amount allowed by applicable law, in which case interest shall accrue at the maximum rate allowed by law.
- 4.8. Set-off Against Sums Owed by Vendor. The State may offset payments owed Vendor under this Agreement by sums the Vendor owes the State or any of its subdivisions in any context. The Vendor agrees that this provision constitutes proper and timely notice under any applicable laws governing offset.
- 4.9. Withholding Payments. In addition to pursuing any other remedy provided herein or by law, the Purchasing Entity may withhold compensation or payments to Vendor, in whole or in part, without penalty or legal liability to the Purchasing Entity or work stoppage by Vendor, in the event Vendor fails to perform pursuant to this Agreement, or fails to provide Deliverables that meet or conform to contractual obligations. No interest shall accrue or be paid to Vendor for withheld sums.
- 4.10. Correction/Cure.
 - 4.10.1. Upon notice of Deficiency in any Deliverable(s), the Vendor shall promptly correct the Deficiency and repair the affected Deliverable(s) and provide the Purchasing Entity with all relevant Documentation.
 - 4.10.2. The Purchasing Entity may correct any Deficiencies with respect to any Deliverable(s) or cure any Vendor breach under this Agreement without prejudice to any other remedy it may have if Vendor fails to correct such Deficiencies as required in this Agreement or if Vendor otherwise fails to perform pursuant to the Agreement. The Purchasing Entity may procure the Deliverable(s) reasonably necessary to correct any Deficiencies or cure any Vendor breach, in which event the Vendor shall reimburse the Purchasing Entity for the actual costs incurred in curing the issue. In addition, the Vendor shall cooperate with the Purchasing Entity or any third parties retained by the Purchasing Entity to cure such breach, including by allowing access to any of the Vendor's pertinent materials, work product, or intellectual property.
- 4.11. Repayment Obligation. In the event that any State of Iowa funds or federal funds are deferred or disallowed as a result of any audits, or found to have been expended in violation of the laws applicable to the expenditure of such funds, and where such findings are due in whole or in part to Vendor's action or omission, Vendor will be liable to the Purchasing Entity for the full amount of any claim disallowed (or the amount of funds expended in violation of such applicable laws) and for all related penalties incurred. If the State of Iowa or any federal agency concludes that Vendor has been paid for any cost that is unallowable, unallocable, or unreasonable under this Agreement, Vendor will be liable to the Purchasing Entity for such cost. Vendor shall pay to the Purchasing Entity all amounts for which the Vendor is liable under this section within twenty (20) business days of receiving the Purchasing Entity's written demand or written notice. The Purchasing Entity may withhold any payment under this Agreement if Vendor fails to timely make any payment required by this section.
- 4.12. Taxes. Vendor shall be responsible for paying any taxes incurred by Vendor in the performance of this Agreement. The State of Iowa, DOM, and the Purchasing Entity are exempt from the payment of sales and other taxes.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**

Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

5. Acceptance Tests and Project Management.

5.1. All Deliverables must undergo the Purchasing Entity's Acceptance Testing as described in this section. If alternative Acceptance Testing processes are described in a Purchasing Instrument(s), the process set forth in the Purchasing Instrument will prevail. After the Vendor completes work on a Deliverable, it must inform the Purchasing Entity that the Deliverable is ready for testing. If the Purchasing Entity requests assistance during testing, the Vendor will assist without levying additional fees or other amounts. The Purchasing Entity will then test the Deliverable(s) to verify that each Deliverable conforms to its Acceptance Criteria. It will then inform the Vendor of Acceptance or Non-Acceptance. If the Purchasing Entity determines Non-Acceptance, the Vendor has ten (10) days to correct the issues and submit the work again for retesting. If the Purchasing Entity again does not provide Acceptance, the Purchasing Entity may pursue any of the following remedies:

- 5.1.1. Require Vendor to correct and repair such Deliverable(s) within such period of time as the Purchasing Entity may specify in a written notice to the Vendor;
- 5.1.2. Refuse to accept such Deliverable(s) without penalty or legal liability and without any obligation to pay any fees or other amounts associated with such Deliverable(s), or receive a refund of any fees or amounts already paid with respect to such Deliverable(s);
- 5.1.3. Accept such Deliverable(s) on the condition that any fees or other amounts payable with respect thereto shall be reduced or discounted to reflect, to the Purchasing Entity's satisfaction, the Deficiencies present therein and any reduced value or functionality of such Deliverable(s), or the costs likely to be incurred by the Purchasing Entity to correct such Deficiencies; or
- 5.1.4. Terminate the applicable Purchasing Instrument or seek any and all available remedies, including damages. Such termination may occur without prior notice or an opportunity to cure.

The Purchasing Entity's right to exercise the foregoing rights and remedies, including termination of the applicable Purchasing Instrument, shall remain in effect through notice of Final Acceptance of all Deliverables. The Vendor's receipt of any notice of Acceptance, including Final Acceptance, with respect to any Deliverable(s) shall not be construed as a waiver of any of the Purchasing Entity's rights to enforce the terms of this Agreement or require performance in the event Vendor breaches this Agreement or any Deficiency is later discovered with respect to such Deliverable(s).

5.2. Project Management and Reporting.

- 5.2.1. *Vendor or Project Manager.* To the extent that a project manager is called for in a Purchasing Instrument, the Vendor must obtain the Purchasing Entity's approval of a designated project manager. The project manager must have authority sufficient to ensure timely performance under the Purchasing Instrument and make binding decisions for the Vendor. Any written commitment by Vendor's project manager and persons designated by them in writing for this purpose, within the scope of this Agreement, shall be binding upon Vendor.
- 5.2.2. *Review Meetings.* Unless a different schedule is established in the Purchasing Instrument, the Vendor's project manager will meet at least monthly with the Purchasing Entity to discuss contractual progress and performance issues. At each review meeting, the Vendor's project manager shall provide a status report, which will describe any problems or concerns

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

encountered since the last meeting. At the next scheduled meeting after which any Party has identified a problem in writing, the Vendor shall provide a report of steps taken to resolve identified problems, together with the anticipated completion dates of such activities. Any Party may recommend alternative courses of action or changes that will facilitate problem resolution. The Vendor shall maintain records of such reports and other communications and provide them to the Purchasing Entity upon request.

5.2.3. *Reports.* Review meeting reports must be in a Purchasing Entity-approved format and include detail concerning the previous period's activities, including problems encountered and their disposition, results of tests, whether or not deadlines were met, the status of services or Deliverables, any problems that may have arisen that need to be addressed before proceeding to the next period's activities, and any other information the Purchasing Entity may request.

5.2.4. *Problem Reporting Omissions.* The Purchasing Entity's receipt of a report that identifies any problems does not relieve the Vendor of any obligation under this Agreement or waive any other remedy available to the Purchasing Entity.

5.2.5. *Vendor Performance Monitoring.*

5.2.5.1. DOM monitors performance through a Vendor scorecard program that collects data on Vendor performance under state contracts gathered through a formal feedback process. Feedback may address cost, delivery and support, flexibility, partnership, and security and compliance. Performance data may include the Vendor's effectiveness in meeting contract obligations, service level agreements, project management requirements, and risk management protocols.

5.2.5.2. Vendors have access to their scorecard results and the methodology by which they are calculated. Scorecards are typically issued annually during the term of the contract. DOM reserves the right to publicly post vendor scorecard results, except where a low score is anticipated, in which case the Vendor will be notified in advance and given the opportunity to appeal through DOM's established process for contested cases applicable to vendor appeals in the applicable Iowa Administrative Code.

5.2.5.3. Scorecard performance may be considered in relation to future State purchasing decisions.

5.3. **Accessibility Conformance Report.** For any Deliverable that includes information and communication technology, Vendor shall provide an Accessibility Conformance Report ("ACR") documenting conformance with the Accessibility Standards. An ACR is based on the Voluntary Product Accessibility Template ("VPAT") developed to demonstrate conformance with Section 508 of the Rehabilitation Act. Vendor shall provide the ACR upon delivery of the applicable Deliverable and shall provide an updated ACR upon any material change to the Deliverable's user interface or accessibility-affecting functionality, at least annually during the Term and upon Agreement renewal.

6. **Ownership and Intellectual Property.** The State of Iowa does not seek ownership of Vendor's pre-existing materials or independently developed tools, software, or know-how. However, where such materials are included in or required to use Customer-Owned Deliverables, the State must receive license rights sufficient to use and disseminate the complete Deliverable for its internal, non-commercial purposes.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 6.1. Ownership and Reservation of Rights in Pre-Existing Vendor Materials. Vendor shall retain ownership of all Vendor Materials that: (i) existed prior to the Effective Date of this Agreement; (ii) are independently developed by Vendor outside the scope of this Agreement; or (iii) are general purpose tools, utilities, or other standard functionality not created specifically for the Purchasing Entity. The Purchasing Entity makes no ownership claim to Vendor Materials. Notwithstanding the foregoing, Vendor may transfer ownership rights to pre-existing Vendor Materials where expressly agreed to in writing in a Purchasing Instrument.
- 6.2. Ownership and Assignment of Customer-Owned Deliverables. Vendor hereby irrevocably assigns, transfers, and conveys to the Purchasing Entity all rights, title, and interest in and to Customer-Owned Deliverables. To the extent any Vendor Materials are incorporated into or required to use a Customer-Owned Deliverable, the Vendor shall provide appropriate use rights as described in Section 6.3.
- 6.3. Waiver and Embedded Vendor Materials. To the extent any of Vendor's rights in Customer-Owned Deliverables are not assignable, including moral rights or rights of attribution, Vendor irrevocably waives such rights and agrees not to challenge the Purchasing Entity's ownership. If Vendor Materials are incorporated into or required to use any Customer-Owned Deliverable, Vendor hereby grants the Purchasing Entity a perpetual, irrevocable, worldwide, non-exclusive, royalty-free license to use them solely as part of, or as necessary to use, the Customer-Owned Deliverable.
- 6.4. Information Technology Assurances. Upon request and at no additional cost, Vendor shall execute all documents and take all actions reasonably necessary to perfect the Purchasing Entity's rights in Customer-Owned Deliverables. If, after reasonable efforts, the Purchasing Entity is unable to obtain Vendor's signature on any required filings for intellectual property protection, Vendor hereby irrevocably appoints the Purchasing Entity as its agent and attorney-in-fact to execute and file such documents with the same legal effect as if signed by Vendor.
- 6.5. Rights in Third Party Intellectual Property. For any Third Party Intellectual Property incorporated into Deliverables, Vendor shall secure for the Purchasing Entity license rights consistent with Section 6.3 above, unless otherwise agreed in writing by the Purchasing Entity.
- 6.6. Customer Property. Vendor may have access to Customer Property to the extent necessary to carry out its responsibilities under the Agreement and must comply with any and all the license terms, conditions, or restrictions applicable to any Customer Property.

7. Representations, Warranties, and Covenants.

- 7.1. Non-exclusivity. Unless expressly stated otherwise in a Purchasing Instrument, express remedies in this Section are not exclusive, and the Purchasing Entity preserves all rights to seek any and all remedies available to it under law both during and after expiration or termination of the Agreement or Purchasing Instrument.
- 7.2. Implied Warranties. To the extent applicable, and unless otherwise stated in a Purchasing Instrument, all warranties implied by law are preserved.
- 7.3. Deliverables Free of Deficiencies. Unless stated otherwise in a Purchasing Instrument, the Vendor guarantees that the Deliverables will be free from material Deficiencies and errors and will meet all Acceptance Criteria and express performance criteria. If the Purchasing Entity identifies any material

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

Deficiencies, the Vendor must fix or replace the affected Deliverables at its own expense. The Vendor will assist the Purchasing Entity, promptly report any known issues, and correct Deliverables, even if the Deliverable(s) have been previously accepted.

- 7.4. Quiet Enjoyment. Vendor represents and warrants that: (i) it owns, possesses, holds, and has received or secured all rights, permits, permissions, licenses, and authority necessary to provide Deliverables to the Purchasing Entity hereunder and to assign, grant, and convey the rights, benefits, licenses and other rights assigned, granted, or conveyed to the Purchasing Entity hereunder without violating any rights of any third party; (ii) it has not previously and will not grant any rights in any Deliverables to any third party that are inconsistent with the rights granted to the Purchasing Entity herein; and (iii) the Purchasing Entity shall peacefully and quietly have, hold, possess, use, and enjoy the Deliverables without suit, disruption, or interruption.
- 7.5. Intellectual Property. The Vendor represents and warrants that the Deliverables and the Purchasing Entity's use of the Deliverables for their authorized use will not infringe on any intellectual property rights of third parties. Vendor also ensures there are no known claims of infringement, violation, or misappropriation of intellectual property rights or trade secrets concerning Deliverables. If such claims arise, Vendor will, at its own expense: (i) secure the right or license for the Purchasing Entity to continue using the Deliverables; (ii) replace the problematic parts with an equivalent; (iii) modify or replace the affected portion with a non-infringing alternative; or (iv) refund all fees paid by the Purchasing Entity for the affected Deliverables.
- 7.6. Workmanlike Manner. The Vendor represents, and warrants that all services to be provided under this Agreement or a Purchasing Instrument will be carried out in a workmanlike manner by qualified personnel, and the work must align with the terms of the Agreement and Purchasing Instrument as well as industry standards for similar tasks. In cases where no specification exists, the Parties agree to follow generally accepted industry standards. If the Purchasing Entity identifies services not meeting these standards, the Vendor will re-perform them at no extra cost. The Vendor will refund any fees paid by the Purchasing Entity for any services that were not satisfactorily provided and cannot otherwise be cured.
- 7.7. Compliance with Laws. The Vendor represents and warrants that the Vendor and Vendor-provided Deliverables will at all relevant times comply with all applicable State and federal laws, including, but not limited to, those relating to information and communication technology accessibility requirements, including applicable provisions of Section 508 of the Rehabilitation Act of 1973 and Title II of the Americans with Disabilities Act of 1990, each as amended, including any implementing regulations and successor standards applicable to public entities serving a population of 50,000 or more (collectively, "Accessibility Standards"). At minimum, Vendor shall conform to the Web Content Accessibility Guidelines as adopted or incorporated by applicable law, or any successor guidelines, whichever imposes the greater accessibility requirements.
- 7.8. No Conflicts. Vendor represents, warrants, and covenants that no relationship exists or will exist during the Term of the Agreement between Vendor and the State or any of its divisions or entities that is or may constitute a conflict of interest or appearance of impropriety, or that would conflict in any manner or degree with the performance of its obligations under this Agreement. To the extent applicable, the provisions of Iowa Code Chapter 68B shall apply to this Agreement and any Purchasing Instruments executed hereunder, and Vendor shall not engage in or permit any third party to engage in any conduct that would violate that chapter.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 7.9. Documentation. The Vendor represents and warrants that during the Term, the Documentation will accurately describe the functional and operational characteristics of any Deliverable and that the Documentation is detailed and complete such that it will allow a reasonably skilled operator to use and operate the Deliverables.
- 7.10. Sole Ownership. Vendor represents and warrants that the Purchasing Entity shall acquire sole ownership of all Customer-Owned Deliverables, free from any rights or interests of Vendor or of any third party. Vendor shall not retain any copies of any Customer-Owned Deliverables.
- 7.11. Compliance with Iowa Department of Management Policies. Vendor shall comply with all applicable policies issued by the Iowa Department of Management, as published at <https://policies.iowa.gov> and as may be amended from time to time. Vendor acknowledges that such policies are incorporated herein by reference to the extent applicable to Vendor's performance under this Agreement.

8. Indemnification.

- 8.1. Indemnification Generally. Vendor shall indemnify and hold harmless DOM, the State of Iowa, the Purchasing Entity, and their employees, officers, or representatives ("Indemnitees") from and against any third-party claims, legal actions, judgments, penalties, fines, recoupments, or other costs, including costs of counsel, in any way arising out of Vendor's performance or attempted performance under this Agreement. The Purchasing Entity shall have the right to participate in its own defense through a representative of the Iowa Department of Justice. Settlement offers made on behalf of the applicable Purchasing Entity must be approved by the applicable Purchasing Entity.
- 8.2. Infringement Claim Additional Remedy. If the Deliverables become or are likely to become the subject of a claim, then, in addition to paying any damages and attorney fees as required above, Vendor shall, at its option, either:
 - 8.2.1. Immediately replace or modify the Deliverables, without loss of material functionality or performance, to make them non-infringing, or
 - 8.2.2. Immediately procure for the Purchasing Entity the right to continue using the Deliverables.
- 8.3. Any costs associated with implementing either of the above alternatives will be borne by the Vendor.

9. Termination.

- 9.1. Termination for Cause by the State. DOM may terminate this Agreement, and any Purchasing Entity may terminate a Purchasing Instrument(s) entered into under this Agreement, upon written notice of Vendor's breach of any material term of the Agreement or associated Purchasing Instrument, if the breach is not cured within the time period specified in the notice of breach. In addition, DOM may terminate this Agreement or a Purchasing Entity may terminate an associated Purchasing Instrument without advance notice if:
 - 9.1.1. Vendor makes false statements in connection with the Agreement,
 - 9.1.2. Vendor, its staff, or its subcontractors have engaged in criminal conduct, including fraud, misappropriation, embezzlement, or malfeasance,
 - 9.1.3. Vendor takes any steps, as determined in DOM's or the applicable Purchasing Entity's discretion, towards dissolution or suspension of business,
 - 9.1.4. Vendor's authority to do business here or elsewhere is threatened or lost,

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 9.1.5. Vendor has failed to comply with applicable laws when performing pursuant to the Agreement or Purchasing Instrument,
 - 9.1.6. Vendor's ability to perform is materially impacted by third-party claims of intellectual property violations by Vendor, or
 - 9.1.7. Vendor's actions may expose DOM, the State of Iowa, or a Purchasing Entity to material liability.
- Vendor shall notify DOM or the applicable Purchasing Entity of any events that could give rise to DOM's right to terminate this Agreement or a Purchasing Instrument for cause.
- 9.2. Termination for Cause by Vendor. Vendor may only terminate an applicable Purchasing Instrument or this Agreement upon written notice of the Purchasing Entity's breach of any material term of this Agreement if the breach is not cured within sixty (60) days of the Purchasing Entity's receipt of Vendor's written notice.
 - 9.3. Termination for Convenience. Following thirty (30) days' written notice, a Purchasing Entity may terminate a Purchasing Instrument in whole or in part without cause. DOM may terminate this Agreement in whole or in part upon thirty (30) days' written notice without cause.
 - 9.4. Termination Due to Lack of Funds or Change in Law. Notwithstanding anything in this Agreement to the contrary, DOM may terminate this Agreement or a Purchasing Entity may terminate a Purchasing Instrument, in whole or in part, without penalty or liability and without any advance notice if:
 - 9.4.1. DOM or the Purchasing Entity determines that it has not been appropriated sufficient funds or funds have been reduced, unallocated, or delayed such that DOM or the Purchasing Entity cannot, in the entity's sole discretion, meet its obligations,
 - 9.4.2. DOM or the Purchasing Entity's authority has been withdrawn or materially altered, or its duties, programs, or responsibilities are modified or materially altered, or
 - 9.4.3. there is a judicial decision that materially or adversely affects DOM's or a Purchasing Entity's ability to fulfill obligations under this Agreement or any applicable Purchasing Instrument.
 - 9.5. Limitation of Payment Obligations. If DOM terminates this Agreement or a Purchasing Entity terminates a Purchasing Instrument for cause, DOM or the applicable Purchasing Entity retains the right to contest amounts that remain unpaid as of the date of termination. In all other termination contexts, the Purchasing Entity will pay those amounts due for goods or services accepted by the Purchasing Entity for which the Purchasing Entity is obligated to pay up to the date of termination, to the extent that funds to make these payments are legally available. Payment is contingent upon the submission and acceptance of invoices for the sums due. Under no circumstances will the Purchasing Entity be liable for sums not expressly owed under the terms of the Agreement or a Purchasing Instrument.
 - 9.6. Vendor's Termination or Expiration Duties. As it relates to this Agreement or any associated Purchasing Instrument, upon receipt of a notice of termination, upon expiration, or upon request of DOM or a Purchasing Entity, Vendor must:
 - 9.6.1. cease work under the Agreement or Purchasing Instrument and take all appropriate actions to limit disbursements and minimize costs;
 - 9.6.2. provide a report to the Purchasing Entity addressing the Purchasing Entity's information needs, including the status of all work performed under the Agreement;

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 9.6.3. cease using and return any Customer Property or Customer-Owned Deliverables;
- 9.6.4. comply with the Purchasing Entity's directions concerning Customer Data;
- 9.6.5. return or refund any Purchasing Entity payments for goods or services not provided to the Purchasing Entity;
- 9.6.6. provide all Deliverables to the extent the Purchasing Entity has a property interest in the Deliverable; and
- 9.6.7. continue to perform and provide such goods and/or services under this Agreement as the Purchasing Entity may request for a transition period of up to 365 days from the effective date of such termination or expiration, and collaborate with the Purchasing Entity and any replacement contractor. As part of such request, the Purchasing Entity will inform the Vendor of the number of days needed for transition ("**Transition Period**"). During the Transition Period, the Purchasing Entity agrees to pay the Vendor any fees to which the Vendor would be entitled under this Agreement for goods and/or services performed or provided during such period. In the event the Purchasing Entity's request for transition assistance does not require the Vendor to continue providing all of the goods and/or services under this Agreement or applicable Purchasing Instrument, the Parties will negotiate in good faith a downward adjustment in the fees owed the Vendor.

10. Use of Artificial Intelligence.

- 10.1. Advance Approval for AI Usage. Vendor shall obtain prior written approval from the Purchasing Entity before utilizing artificial intelligence (AI) technologies in the provision of services under this Agreement or Purchasing Instruments entered into pursuant to this Agreement. The Vendor shall clearly identify in writing the specific AI technologies to be employed, their intended functions, and their potential impact on service delivery.
- 10.2. Documentation of AI Utilization. In cases where computer code is generated, written, or modified using AI technologies, the Vendor shall ensure that the sections of code influenced by AI are thoroughly documented with appropriate comments indicating that they are the result of AI utilization. This Documentation shall be provided along with any Deliverables that include AI-derived code.
- 10.3. AI Training Data Usage. The Vendor shall not employ Customer Data or Confidential Data to train AI systems without obtaining prior written approval from the Purchasing Entity. The intended usage of such data for AI training must align with existing data usage rights, and the Vendor shall ensure that data privacy and security are maintained throughout the process.
- 10.4. Data Normalization to Prevent Discrimination. The Vendor shall include within a submitted Plan of Action and Milestones (POAM) a detailed outline of the measures to be taken for data normalization in AI training. This normalization process shall be designed to prevent algorithmic discrimination and ensure fair and equitable outcomes.
- 10.5. Evaluation of Third-Party AI Offerings. Should the Vendor intend to employ third-party AI offerings in the execution of this Agreement or Purchasing Instruments entered into pursuant to this Agreement, the Vendor must provide a comprehensive explanation of how such AI technologies have been trained to avoid algorithmic discrimination, safeguard data privacy, and ensure system safety.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

and effectiveness. The Vendor shall also provide advanced notice and clarification to any individuals whose data might be used for future AI training.

- 10.6. Human Alternatives and Fail-Safe Mechanisms. In instances where AI technologies fail to adequately fulfill the service requirements, the Vendor shall ensure the provision of human-operated alternatives that are capable of meeting the needs of the circumstance. These alternatives shall be readily available to ensure seamless service continuity.
- 10.7. Human Vetting of AI Output. Prior to finalizing any output generated by AI technologies, the Vendor shall subject such output to thorough human evaluation and interaction. This evaluation shall assess the accuracy, relevance, and appropriateness of AI-generated content, ensuring the delivery of high-quality, reliable results.
- 10.8. Compliance and Reporting. The Vendor shall adhere to all applicable laws, regulations, and standards governing the use of AI technologies in the context of the Agreement. The Vendor shall provide regular reports to the Purchasing Entity detailing the usage, performance, and outcomes of AI technologies as per the terms of this clause.

11. General Provisions.

- 11.1. Immigration Status. The Vendor is responsible for ensuring compliance with all Visa requirements. The Purchasing Entity requires the Vendor to conduct E-Verify employment-eligibility verifications of Vendor personnel working under this Agreement at the Vendor's cost. The Vendor shall provide to the Purchasing Entity with the E-Verify results as directed.
- 11.2. No Publicity. The Vendor is prohibited, both during the term of the Agreement and after the Agreement's termination or expiration, from publicizing this contractual arrangement relationship or in any way using, as applicable, DOM's or the Purchasing Entity's name, logo, or other identifying information without prior written consent.
- 11.3. Independent Contractor. The Vendor is an independent contractor performing services for a Purchasing Entity and shall not be considered an employee, partner, or agent of the Purchasing Entity. Vendor personnel are not employees of the State of Iowa simply by virtue of work performed under this Agreement. The Vendor is responsible for all taxes, licenses, insurance, and other obligations arising from their status as an independent contractor.
- 11.4. Amendments. This Agreement or any Purchasing Instrument may be amended from time to time by mutual written consent of the Parties. The Parties expressly agree that no amendments or modifications to this Agreement shall be affected through transactional documents. Notwithstanding the above, specific Purchasing Instruments may modify the terms of the Agreement as necessary to affect the Parties' intent with respect to such Purchasing Instrument. However, any such modifications shall be limited to the scope of the Purchasing Instrument.
- 11.5. No Third-Party Beneficiaries. There are no intended third-party beneficiaries to this Agreement.
- 11.6. Choice of Law and Forum. This Agreement shall be governed by the laws of the State of Iowa, without giving effect to the choice of law principles of Iowa law. Any litigation in connection with this Agreement shall be brought and maintained in the state or federal courts sitting in Polk County, Iowa.

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 11.7. Assignment and Delegation. This Agreement may not be assigned, transferred, or conveyed in whole or in part without the prior written consent of the other Party, except that DOM may assign, transfer, or convey this Agreement, in whole or in part, to any entity that succeeds its duties hereunder or otherwise assumes responsibility for functions or duties currently assumed by DOM.
- 11.8. Use of Third Parties. None of the Deliverables to be provided by Vendor pursuant to this Agreement shall be subcontracted or delegated to any third party without the prior written consent of a Purchasing Entity. Such consent shall not be deemed in any way to provide for the incurrence of any additional obligation of a Purchasing Entity, whether financial or otherwise. Any subcontract to which a Purchasing Entity has consented shall be in writing and shall in no way alter the terms and conditions of this Agreement. All subcontracts shall be subject to the terms and conditions of this Agreement and to any conditions of approval that a Purchasing Entity may deem necessary.
- 11.9. Integration. This Agreement supersedes former agreements for the goods and/or services addressed in the Agreement and represents the entire agreement between the Parties. Neither Party is relying on any representation that may have been made that is not included in this Agreement. No click-through, or other end user terms and conditions or agreements required by the Vendor ("Additional Terms") that are not part of this Agreement provided with any Services hereunder shall be binding on DOM or the Purchasing Entity, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.
- 11.10. Waiver. The parties may agree in writing to waive some aspect of Vendor performance. Failure by one Party to require performance under the Agreement by the other Party does not affect the right to enforce the Agreement's terms or claim breach concerning subsequent Agreement compliance issues.
- 11.11. Notices. Any legal notices required by the Agreement, or a Purchasing Instrument, shall be given in writing by registered or certified mail with proof of receipt, or overnight delivery, which shall be addressed to each party's Notice Address. To the extent a Purchasing Instrument is executed by a Purchasing Entity other than DOM, the Vendor shall additionally notice the Purchasing Entity at the billing address set forth on the applicable Purchasing Instrument. From time to time, the parties may change the name and address of a party designated in the Notice Address. Such changes shall be in writing to the other party. Notices shall be deemed to have been provided at the time it is actually received in the case of hand delivery; within one day in the case of overnight delivery; or within five days after it is deposited in the U.S. Mail.
- 11.12. Cumulative Rights. The various rights, powers, options, elections, and remedies of DOM or any Purchasing Entity provided for in this Agreement shall be construed as cumulative.
- 11.13. Severability. If any provision of this Agreement is determined by a court to be invalid or unenforceable, such determination shall not affect the validity or enforceability of any other part or provision of this Agreement.
- 11.14. Time is of the Essence. Time is of the essence with respect to the Vendor's performance of its obligations under this Agreement. Vendor shall ensure that all Vendor Personnel providing services and Deliverables hereunder are responsive to the Purchasing Entity's requirements and requests in all respects, including in accordance with any specific timelines identified in a duly executed Purchasing Instrument.

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 11.15. Authorization. The Vendor represents and warrants that it has the right, power, and authority to enter into and perform its obligations under this Agreement and that it has taken all requisite action to approve the execution, delivery, and performance of this Agreement, and this Agreement constitutes a legal, valid, and binding obligation of the Vendor, enforceable in accordance with its terms.
- 11.16. Successors in Interest. All terms, provisions, and conditions of the Agreement shall be binding upon and inure to the benefit of the Parties hereto and their respective successors, assigns, and legal representatives.
- 11.17. Records Retention and Access. The Vendor shall maintain records that sufficiently and properly document the Vendor's performance under this Agreement, including records that document all fees and other amounts charged during the Term of this Agreement, for a period of at least five years following the later of the date of final payment, termination, or expiration of this Agreement, or the completion of any audit. The Vendor shall permit the Auditor of the State of Iowa or any authorized representative of the Purchasing Entity, and where federal funds are involved, any authorized representative of the United States government, at no charge, to access and examine, audit, excerpt, and transcribe any pertinent records of the Vendor, however stored, relating to the Vendor's performance under this Agreement. The Vendor shall require Vendor contractors to agree to the same provisions as set forth in this subsection.
- 11.18. Right of Inspection/Vendor Compliance. The Purchasing Entity may inspect the Vendor's books and records at reasonable times in order to monitor the performance of this Agreement or a Purchasing Instrument, including but not limited to any request that the Vendor provide a copy of its affirmative action program, containing goals and time specifications in accordance with Iowa Admin. Code ch. 11-121. All subcontracts shall contain provisions that allow the same. The Vendor shall promptly comply with and correct any deficiencies noted in any audit and promptly implement any recommendations requested by the Purchasing Entity. The Vendor shall not impose any charge or fee in connection with any such audit.
- 11.19. Headings and Captions. The Parties acknowledge that the headings and captions used in this Agreement are for convenience and reference purposes only. They are not intended to have any legal or substantive significance or alter the meaning or interpretation of the provisions they precede.
- 11.20. Multiple Counterparts and Electronic Signatures. This Agreement may be executed in several counterparts, each of which shall be considered an original and all of which, when taken together, shall constitute one contract binding on all Parties. The Parties agree to accept electronic signatures in lieu of "wet" signatures on Agreement documents in accordance with Iowa Code chapter 554D or other applicable law.
- 11.21. Not a Joint Venture. Nothing in this Agreement shall be construed as creating or constituting a partnership, joint venture, or other association of any kind implying the establishment of an agent/principal relationship between the Parties.
- 11.22. Attachments. The Parties agree that if any document is attached hereto by the Parties, and referred to herein, then the same shall be deemed incorporated herein by reference as if fully set forth herein.

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 11.23. Further Assurances. Each party shall do and perform, or cause to be done and performed, all such further acts and things, and shall execute and deliver all such other agreements, certificates, instruments and documents, as the other party may reasonably request in order to carry out the intent and accomplish the purposes of this Agreement.
- 11.24. Force Majeure. If one Party is unable to fulfill its obligations under this Agreement due to circumstances beyond its control, including unforeseeable events that no one could have predicted or prevented, such as acts of God, war, civil disturbances, or other catastrophic events, that Party will not be considered in breach of this Agreement. These circumstances must be abnormal and unforeseeable, and the Party affected must have taken all necessary precautions to prevent them. However, financial difficulties, legal restrictions, strikes, labor unrest, supply chain disruptions, internet failure, power outages, hacker attacks, viruses, and Security Breaches are not considered force majeure events. If a delay or inability to perform is caused by a subcontractor hired by the Party, the Party cannot use force majeure as an excuse unless the subcontractor is also affected by a force majeure event. If a force majeure event affects the Party's performance, the Party will make its best efforts to provide an alternative, if possible, comparable solution. The Purchasing Entity will determine whether the alternative solution is comparable. The Party invoking force majeure must immediately inform the other Party about the event causing the delay and the reasons behind it. Both Parties will work together to minimize the impact of the delay and the scope of work affected by the unforeseen events. If the Vendor's performance obligations have specific deadlines, those deadlines will be extended by the amount of time lost due to the force majeure event.

11.25. Administrative Fees and Reporting.

- 11.25.1. Vendor shall provide one percent (1.00%) administrative fee on all sales made through this Agreement, without affecting authorized prices/rates. This one percent (1.00%) administrative fee shall be paid quarterly to the Iowa Department of Management, Attn: Chief Financial Officer, at the billing address located in CD&E section. Payment shall be made in accordance with the following schedule:

<u>Period End</u>	<u>Reporting and Fee Due</u>
September 30 (Q1)	October 31
December 31 (Q2)	January 31
March 31 (Q3)	April 30
June 30 (Q4)	July 31

- 11.25.2. The Vendor shall submit a quarterly report via email to **ITContracts@dom.iowa.gov** detailing all sales in the State of Iowa and identifying the Purchasing Entity, the Purchasing Instrument number, and the State of Iowa Contract number. The quarterly sales report is due on the dates listed above.

- 11.26. Title to Property. Title to all property furnished by the Purchasing Entity to the Vendor to facilitate the performance of this Agreement and any Customer-Owned Deliverables shall remain the sole property of the Purchasing Entity, as applicable. The Vendor shall be responsible for the proper

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

custody and care of any such property and may not encumber such property or otherwise use such property for monetary gain. All such property shall only be used by the Vendor for purposes of fulfilling its obligations under this Agreement and shall be returned to the Purchasing Entity at the conclusion of the Agreement.

- 11.27. Exclusivity. This Agreement is not exclusive. DOM or the Purchasing Entity may obtain similar or identical goods or services from other vendors.
- 11.28. Award of Related Agreements. A Purchasing Entity may undertake or award supplemental or successor agreements for work related to this Agreement or under a Purchasing Instrument. Vendor shall cooperate fully with Authorized Contractors who may be engaged by a Purchasing Entity in connection with a Purchasing Instrument.
- 11.29. Attorney's Fees and Costs. If the Vendor is found to be in breach of its obligations under this Agreement by a court or tribunal of competent jurisdiction or if the Vendor fails to successfully defend against any legal action arising out of or relating to this Agreement, the Vendor shall be liable for and shall promptly reimburse the Purchasing Entity for all reasonable attorney's fees, court costs, and any other related expenses incurred by the Purchasing Entity in enforcing its rights or remedies under this Agreement.
- 11.30. Survival. Expiration or termination of this Agreement or a Purchasing Instrument for any reason will not release either Party from any duties, liabilities, or obligations that expressly survive termination or that by their very nature would be intended to be applicable following expiration or termination of the Agreement. Provisions that expressly survive include:
 - 11.30.1.1. Section 3.3 (Source Code Release and License Rights);
 - 11.30.1.2. Section 4 (Compensation and Additional Rights and Remedies);
 - 11.30.1.3. Section 6 (Ownership and Intellectual Property);
 - 11.30.1.4. Section 7 (Representations, Warranties, and Covenants);
 - 11.30.1.5. Section 8 (Indemnification);
 - 11.30.1.6. Section 9 (Term and Termination);
 - 11.30.1.7. Section 10 (Use of Artificial Intelligence);
 - 11.30.1.8. Section 11 (General Provisions); and
 - 11.30.1.9. Attachment B (Data Protection Addendum).

12. Insurance.

- 12.1. Insurance Requirement. The Vendor shall, at its sole expense, maintain in full force and effect, insurance covering its work of the type and in amounts required by this attachment. Vendor's insurance shall, among other things, insure against any loss or damage resulting from or related to Vendor's performance of the Agreement, regardless of the date the claim is filed or expiration of the policy. All insurance policies required by this Exhibit shall: (a) remain in full force and effect for the entire Term of the Agreement; and (b) not be reduced, changed (to the detriment of DOM, the Purchasing Entity, or any governmental entities), or canceled (without being simultaneously replaced by another policy meeting the requirements of this section).

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
 Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 12.2. Exclusion. The following insurance obligations do not apply in any setting in which a Vendor only provides licensed software to the Purchasing Entity and does not have access to Customer Data through that relationship.
- 12.3. Insurance Policies. Unless otherwise requested by the Purchasing Entity, the Vendor shall cause to be issued insurance policies with the coverages set forth below:

<u>Type of Insurance</u>	<u>Limit</u>	<u>Amount</u>
General Liability (including contractual liability) written on an occurrence basis	General Aggregate	\$2 million
	Products –	
	Comp/Op Aggregate	\$1 million
	Personal injury	\$1 million
Excess Liability, umbrella form	Each Occurrence	\$1 million
	Aggregate	\$1 million
Technology Errors and Omissions Insurance	Each Occurrence	\$5 million
	Aggregate	\$5 million
Workers Compensation and Employer Liability	As Required by Iowa law	\$2 million
Cyber Liability / Network Security	Each Occurrence	\$5 million
	Aggregate	\$5 million

- 12.4. Claims Provision. All insurance policies required by this Exhibit, with the exception of the policy for Errors and Omissions Insurance, must provide coverage on an “occurrence basis” for all claims arising from activities occurring during the term of the policy, regardless of the date the claim is filed or expiration of the policy. The policy for Errors and Omissions Insurance will provide coverage on a “claims made” basis, provided, however, that such policy includes an extended reporting period or tail coverage acceptable to the Purchasing Entity.
- 12.5. Certificates of Coverage. The Vendor shall submit certificates of the insurance, which indicate coverage and notice provisions as required by this Contract, to the Agency upon execution of this Contract. Send the Certificate of Insurance (COI) to the DOM contract email address: **ITContracts@dom.iowa.gov**. Include in the COI the following additions:

COI - Description of Operations box shall state:

The State of Iowa and the Iowa Department of Management are named as additional insured. No insurance cancellation shall be made without at least thirty (30) days prior written notice to the State of Iowa and the Iowa Department of Management.

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

COI - The Certificate Holder box shall state:

State of Iowa - Department of Management

200 East Grand Avenue

Des Moines, IA 50309

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

Attachment B - Data Protection Addendum

1. Definitions:

- 1.1. **“Security Breach”** means the loss of control, compromise, unauthorized use, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses personally identifiable information; or an authorized user accesses Customer Data for a reason other than an authorized purpose.
- 1.2. **“Security Incident”** means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of (1) Customer Data, and/or (2) an information system or the information the system Processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

2. Confidentiality

- 2.1. Customer Data. The Purchasing Entity owns and has exclusive rights to all Customer Data. Vendor must treat all Customer Data as Confidential Information, keep it secure, and not disclose or use it for any purpose other than providing goods or services under the Agreement. All uses for commercial or political purposes are strictly forbidden. Vendor must comply with any restrictions on use or disclosure outlined in the Agreement or applicable law. Vendor may only retain Customer Data for purposes of performing pursuant to the Purchasing Instrument or by prior written approval of the Purchasing Entity. The Vendor may be held civilly or criminally liable for improper use or disclosure of Customer Data. The Vendor shall not link any data provided by DOM or a Purchasing Entity with any other data systems or data sets without prior written permission from the applicable entity.
- 2.2. Vendor Confidential Information. Unless otherwise required by applicable law, the Purchasing Entity will not intentionally disclose Vendor’s Confidential Information to a third party (excluding the Purchasing Entity’s Authorized Contractors) without the Vendor’s prior written consent.
- 2.3. Return or Destruction. Upon completion of duties under this Agreement or upon the specific direction of either party, the other party shall return or destroy Confidential Information and/or Customer Data and not retain any copies thereof, subject to any retention obligations imposed by law. If immediate destruction is not possible, the party retaining such information shall return or destroy the retained information as soon as feasible and shall certify that the retained information will be safeguarded to prevent unauthorized disclosures until it has been purged. Once all Confidential Information and/or Customer Data has been completely purged, the party purging the information shall provide certification of destruction in accordance with methods approved by the National Institute of Standards and Technology.
- 2.4. Compelled Disclosures. In the event that a subpoena or other legal process is served upon either party for Customer Data held by Vendor or for Vendor Confidential Information held by a Purchasing Entity, the party shall promptly notify the other party and cooperate in any lawful effort to defend against the disclosure.
- 2.5. Open Records and Electronic Discovery Requests. Vendor must assist the Purchasing Entity by providing information needed to comply with open records laws (including Iowa Code Chapter 22) or in connection with any legal process or proceeding. Vendor’s assistance in this regard must be provided timely and designed to meet the timing obligations imposed by law. Vendor will ensure

Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

Customer Data is stored and maintained so as to avoid spoliation or other electronic discovery issues. For purposes of Iowa Code Chapter 22, Vendor is not the lawful custodian of Customer Data it holds, and Vendor shall not respond to a records request for Customer Data but shall promptly route the request to the Purchasing Entity and assist the Purchasing Entity's response.

3. Security/Privacy.

- 3.1. Data Protection. Vendor shall safeguard the confidentiality, integrity, and availability of Customer Data, Customer Property, and the Deliverables. In so doing, Vendor shall implement and maintain reasonable and appropriate administrative, technical, and physical security measures to safeguard against unauthorized access, disclosure, theft, or modification of Customer Data, Customer Property, and Deliverables.
- 3.2. Compliance with Security Plan. Vendor represents and warrants that it will adhere to the cybersecurity plan adopted pursuant to the Vendor Security Framework identified in the CD&E. Vendor will ensure that its internal policies, procedures, and practices align with the objectives and requirements set forth in the cybersecurity plan and the Vendor Security Framework. The identified Vendor Security Framework may be changed or updated from time to time by mutual agreement of the Parties.
- 3.3. Compliance Reporting. Annually during the Term, a Purchasing Entity may request, and Vendor shall provide, evidence of compliance with the Vendor's Security Framework.
- 3.4. Encryption. Customer Data shall be encrypted at rest and in transit with controlled access, and the Deliverables shall use TLS 1.2 or higher. Unless otherwise expressly provided herein or otherwise agreed to by the Parties in writing, Vendor is responsible for encryption of Customer Data in its possession. Additionally, Vendor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in Federal Information Processing Standards (FIPS) 140-3, Security Requirements for Cryptographic Modules for all Customer Data, unless the Purchasing Entity approves in writing the storage of Customer Data on a portable device that does not satisfy these standards.
- 3.5. CONUS Obligation. Access, storage, Processing, transmission, retention, or other maintenance of Customer Data at rest and all backups shall occur solely in the continental United States of America. Vendor shall not allow Vendor personnel to access, store, Process, or retain Customer Data on any portable devices, including personal computers, tablets, or cell phones, except to the extent such devices are used and permanently stored or backed up at all times only in the continental United States of America.
- 3.6. Import and Export of Data. Purchasing Entity must have the ability at all times to extract Customer Data and other information from any Vendor systems housing such information or data. Vendor must assist with such extracts when necessary, must not interfere with such extracts, must ensure extracts are provided at no additional charge to the Purchasing Entity, and must make sure that data can be exported in a commercially reasonable format so that the Purchasing Entity can then import data into other systems. Regarding exporting data and information, the Vendor must ensure that the Purchasing Entity receives the requested data or information within seven days of making a request. The format of the exported data should be as specified by the Purchasing Entity or, if not feasible, in a commercially reasonable format.
- 3.7. Security Audits. During the Term, DOM or the Purchasing Entity may perform security audits of Vendor's environment used to provide Deliverables. Vulnerabilities will be measured using standards

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

set forth at <https://cve.mitre.org/>. Vendor agrees to remediate vulnerabilities identified through such audits within the following timeframes: (a) Critical vulnerabilities: 15 days; (b) Serious vulnerabilities: 30 days.

3.8. Access to Security Logs and Reports. Vendor shall provide security logs and reports to DOM and/or the Purchasing Entity in a mutually agreeable format upon request. Such reports shall include, at minimum, latency statistics, user access summaries, user access IP address summaries, and user access history and security logs related to Customer Data.

3.9. Personnel Safeguards.

3.9.1. *Background Checks.*

3.9.1.1. *Minimum Requirements.* Vendor shall comply with its internal background check policies. Where Vendor does not have an internal background check policy, or in the event Vendor's background check policy is inadequate based on the nature of Customer Data stored or processed by Vendor, Vendor agrees to comply with DOM background check policy. Vendor shall provide DOM and the Purchasing Entity with these background check results in a mutually agreeable form and manner prior to Vendor staff performing services pursuant to this Agreement or a Purchasing Instrument. In the event of an adverse finding, Vendor personnel may be disqualified from performing services under the Agreement in the sole discretion of the applicable Purchasing Entity.

3.9.1.2. *Costs.* Vendor is responsible for all costs associated with any Vendor personnel background checks, regardless of who performs the background checks.

3.9.1.3. *Additional Screening.* If any Vendor personnel will access, or have the ability to access, data that is subject to federal regulatory requirements (including, but not limited to, data regulated under the Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS) Security Policy, Internal Revenue Service (IRS) Publication 1075, or other federal data protection laws), then the Vendor shall ensure that such personnel undergo background checks in compliance with all applicable federal regulations prior to the commencement of any engagement involving access to such data.

These background checks may include, as required by the applicable regulations, a work history review, financial review, state or local criminal history check, and a national criminal history check through the Federal Bureau of Investigation (FBI). Vendor personnel may also be required to authorize the release of background check results, including those from the FBI, to DOM, the Purchasing Entity, or other applicable governmental authorities.

Such background checks may be conducted by the Purchasing Entity, DOM, or their Authorized Contractors, or may be required to be performed by Vendor in accordance with applicable federal standards. The results shall be provided in a mutually agreeable form and manner prior to access to the regulated data.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**

Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

DOM and the Purchasing Entity reserve the right to require additional background screening during the engagement, consistent with applicable law and regulation.

3.9.1.4. *Right to Remove Individuals.* The Purchasing Entity and DOM shall have the right at any time to require that the Vendor remove from interaction with the Purchasing Entity or DOM, as applicable, any Vendor representative who the Purchasing Entity or DOM believes is detrimental to its working relationship with the Vendor. The Purchasing Entity or DOM will provide the Vendor with notice of its determination and the reasons it requests the removal. If the Purchasing Entity or DOM signifies that a potential security violation exists with respect to the request, the Vendor shall immediately remove such individual. The Vendor shall not assign the person to any aspect of this Agreement or future work orders without the Purchasing Entity's or DOM's consent.

3.9.2. *Security Awareness Training.* Vendor personnel providing services to DOM or a Purchasing Entity are required to attend annual security awareness training addressing the importance of securing, safeguarding, and otherwise appropriately handling Customer Property, including Customer Data. Any such security awareness training shall minimally conform with applicable DOM Security Awareness Training policies or requirements. Where a Purchasing Instrument requires compliance with training requirements imposed by federal partners, the Vendor agrees to comply with the more stringent training requirements.

3.9.3. *Separation of Job Duties and Non-disclosure.* Vendor shall monitor and enforce separation of job duties, and limit access to and knowledge of Customer Property and Customer Data to those Vendor personnel to which such access and knowledge is necessary to provide the Deliverables hereunder. Vendor personnel may be required to sign the Purchasing Entity's standard confidentiality or non-disclosure agreement(s), or other confidentiality or non-disclosure agreement(s), including as may be required by applicable law, rule, regulation, or policy.

4. Security Incidents and Breaches.

4.1. Security Incident or Data Breach Notification:

4.1.1. *Reporting Requirements.* Vendor must report Security Incidents and Security Breaches (collectively "Security Events") to the contact identified in the applicable Purchasing Instrument(s) as well as to the State of Iowa Security Operations Center ("SOC"):

Email: soc@iowa.gov

Local: 515-281-4762 (4SOC)

4.1.2. *Notification Timeframes.* The Vendor shall notify the SOC of Security Events within the shorter of (a) 72 hours, (b) the timeframe listed in the Purchasing Instrument, or (c) the timeframe imposed by applicable law. Vendor shall only delay notification to DOM and the Purchasing Entity of a Security Event when required to do so by applicable law.

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**

Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

- 4.2. Investigations in Response to Security Events. The Vendor agrees at its sole expense to take all steps necessary to promptly remedy any Security Event and to fully cooperate with DOM and the Purchasing Entity in investigating and mitigating any damage from such Security Events. Upon notice of any Security Event, the Vendor will immediately institute appropriate controls to maintain and preserve all electronic evidence relating to the Security Event. As soon as practicable during the investigation, the Vendor will deliver to the SOC a Security Event assessment and the Vendor's plans for future mitigation. When DOM notifies Vendor that the investigation into any Security Event has concluded, Vendor will deliver to DOM and the Purchasing Entity a final root cause assessment and future incident mitigation plan as soon as practicable. Vendor agrees that it will not notify any regulatory authority relating to any Security Event unless DOM and the Purchasing Entity specifically request Vendor do so in writing, or unless otherwise required to do so by applicable law. Vendor's reports, assessments, and other communications to the State concerning Security Events are made in furtherance of Iowa Code section 8.97, shall be treated by Vendor as confidential, and shall not be disclosed by Vendor except as required by law or as authorized by the State in writing.
- 4.3. Consumer Notification Obligation. Vendor shall be responsible for all applicable consumer notification requirements in the event of a Security Event caused in whole or in part by Vendor.
- 4.4. Exposure for Damages related to Security Events. Vendor shall be responsible for all damages arising directly or indirectly, in whole or in part, out of any Vendor act or omission related to a Security Event. Any such damages shall be construed as direct damages for purposes of this Agreement, and such damages expressly include any costs, expenses, damages, fines, legal fees (including the time and expense of the Iowa Attorney General's Office), and court costs related to the Security Event.

5. Disaster Recovery and Business Continuity.

- 5.1. Creation, Maintenance, and Testing. The Vendor shall maintain a Business Continuity and Disaster Recovery Plan for the Deliverables ("**Plan**"), test the Plan at least yearly, and implement the Plan in the event of any unplanned interruption. The Plan, compliance history, and testing results will be forwarded to the Purchasing Entity upon request. Throughout the Term, the Vendor shall maintain disaster avoidance procedures designed to safeguard the Customer Data, the data processing capability, and the availability of the Deliverables. Additional disaster recovery and business continuity requirements may be set forth in individual Purchasing Instruments.
- 5.2. Activation of Plan. The Vendor shall immediately notify DOM and the Purchasing Entity of any disaster or other event that results in the activation of the Plan. If Vendor fails to reinstate the Deliverables impacted by any such disaster within the periods of time set forth in the Plan, DOM or Purchasing Entity, as applicable, may immediately terminate this Agreement or applicable Purchasing Instrument as a non-curable breach and without any penalty or liability. Termination under this section is in addition to any other remedies available hereunder. Force Majeure provisions of the Agreement shall not limit Vendor's obligations under this section.
- 5.3. Backup and Recovery. Except as otherwise set forth in a Purchasing Instrument or Service Level Agreement, the Vendor shall maintain a contemporaneous backup of Customer Data such that the data shall be restored within twenty-four hours at any point in time. Additionally, unless otherwise provided in a Purchasing Instrument or applicable Service Level Agreement, Vendor shall store a backup of Customer Data in a facility at least as secure as the production facility no less than daily, and maintain the security of Customer Data consistent with the security requirements set forth in this Agreement. Backups of Customer Data shall not be considered in calculating storage used by

**Participating Addendum Number 2026-BUS-7678 for
Cloud and Software Solutions**
Between **the State of Iowa – Department of Management** and
Carahsoft Technology Corporation

DOM or a Purchasing Entity in the event that fees are calculated based on storage used or amount of data transfer under the Agreement. All costs of data restoration shall be borne by the Vendor.

6. Survives Termination. Vendor's duties, obligations, and liabilities as set forth in this Data Protection Addendum shall survive termination of this Agreement.

Contract # LS4992

STATE OF UTAH COOPERATIVE CONTRACT

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

<u>DLT Solutions LLC</u>		
Name		
<u>2411 Dulles Corner Park</u>		
Address		
<u>Herndon</u>	<u>VA</u>	<u>20171</u>
City	State	Zip

LEGAL STATUS OF CONTRACTOR

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

Contact Person Adam Pritchard Phone # 703-773-8988 Email adam.pritchard@dlt.com
 Vendor #94622A Commodity Code #92005

2. CONTRACT PORTFOLIO NAME: Cloud and Software Solutions
3. PROCUREMENT: This Contract is entered into as a result of Solicitation #BP24-1.
4. CONTRACT PERIOD: Effective Date: 9/16/2026 Termination Date: 9/15/2036 unless terminated early or extended in accordance with the terms and conditions of this Contract. Renewal options (if any): None.
5. Prompt Payment Discount (if any): None. Price Guarantee Period (if any): Minimum Percentage Discount: Life of the contract
 Direct Service Provide Pricing: 1 year.
6. ATTACHMENT A: NASPO ValuePoint Master Agreement Terms and Conditions
 ATTACHMENT B: Scope of Work
 ATTACHMENT C: Pricing Catalog
 ATTACHMENT D: Contractor's Response to Solicitation
 ATTACHMENT E: End User Agreements
 ATTACHMENT F: 3rd Party Provider Agreement Template

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

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- 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.
9. Each person signing this Contract represents and warrants that he/she is duly authorized and has legal capacity to execute and deliver this Contract and bind the parties hereto. Each signatory represents and warrants to the other that the execution and delivery of the Contract and the performance of each party's obligation hereunder have been duly authorized and that the Contract is a valid and legal Contract binding on the parties and enforceable in accordance with its terms.
- IN WITNESS WHEREOF, the parties sign and cause this Contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 4 above.

CONTRACTOR

DocuSigned by:

Contractor's Signature

Steve Wells

Print Name

Vice President, Operations

Title

12/2/2025

Date

DocuSigned by:

C38BE9DAC528424...

Director, Division of Purchasing

12/3/2025

Date

ATTACHMENT A

NASPO VALUEPOINT MASTER AGREEMENT TERMS AND CONDITIONS

I. Definitions

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

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

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

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

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

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

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

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

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

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

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

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

- 1.9 Hardware** is defined as any physical component that make up a computer, electronic, or IT infrastructure system.
- 1.10 High Risk Data** is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("High Impact Data"). This refers to the Data for which the loss of confidentiality, integrity, or availability could have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- 1.11 Infrastructure as a Service (IaaS)** Further defined in section A.1. IaaS as used in this Master Agreement is defined as the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
- 1.12 Intellectual Property** means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.
- 1.13 Lead State** means the State centrally administering any resulting Master Agreement(s) who is a party to this Master Agreement.
- 1.14 Low Risk Data** is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").
- 1.15 Master Agreement** means the underlying agreement executed by and between the Lead State, acting in cooperation with NASPO ValuePoint, and the Contractor, as now

or hereafter amended.

- 1.16 Moderate Risk Data** is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“Moderate Impact Data”).
- 1.17 NASPO ValuePoint** is a division of the National Association of State Procurement Officials (“NASPO”), a 501(c)(3) corporation. NASPO ValuePoint facilitates administration of the NASPO cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (*i.e.*, colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports, as well as other contract administration functions as assigned by the Lead State.
- 1.18 Non-Public Data** means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.
- 1.19 Order or Purchase Order** means any Purchase Order, sales order, contract or other document used by a Purchasing Entity to commit funds in exchange for a Contractor’s delivery of one or more Products under this Master Agreement.
- 1.20 Participating Addendum** means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any additional Participating Entity-specific language or other requirements (*e.g.*, ordering procedures specific to the Participating Entity, entity-specific terms and conditions, etc.).
- 1.21 Participating Entity** means a state (as well as the District of Columbia and US territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states properly authorized to enter into a Participating Addendum, that has executed a Participating Addendum.
- 1.22 Participating State** means a state that has executed a Participating Addendum or has indicated an intent to execute a Participating Addendum.
- 1.23 Personal Data** means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (*e.g.*, Social Security, driver’s license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person. Federal Tax Information (FTI) as defined by the federal government Internal Revenue Service Publication 1075 (as updated, replaced, or amended over time).
- 1.24 Platform as a Service (PaaS)** Further defined in section A.1. PaaS as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment

configurations

- 1.25 Product or Products and Services** means any equipment, software (including Embedded Software), documentation, service, or other deliverable supplied or created by the Contractor pursuant to this Master Agreement. The term Product includes goods and services.
- 1.26 Protected Health Information (PHI)** means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual
- 1.27 Purchasing Entity** means a state (as well as the District of Columbia and US territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states if authorized by a Participating Addendum, that issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.
- 1.28 Service Level Agreement or SLA** means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) the amount of time required for notice by the provider to the public jurisdiction of upcoming changes, (3) security notice requirements, (4) timeframes for response to operational problems and failures, (5) description of service quality, (6) identification of roles and responsibilities, (7) remedies, such as credits, and (8) an explanation of how remedies or credits are calculated and issued.
- 1.29 Software as a Service (SaaS)** Further defined in section A.1. SaaS as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure'). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings
- 1.30 Solicitation** means the Solicitation resulting in this Master Agreement.
- 1.31 Subcontractor** includes contractors, manufacturers, distributors, suppliers, or consultants, at any tier, that are under the direct or indirect control or responsibility of Contractor, including a person or entity that is, or will be, providing Product or Products and Services pursuant to this Master Agreement.

II. Term of Master Agreement

- II.1 Initial Term.** The initial term of this Master Agreement is for ten (10) years. The Lead State may, prior to execution, adjust the effective date or duration of the initial term or renewal period of any Master Agreement for the purpose of making the Master Agreement coterminous with others.
- II.2 Amendment Limitations.** The terms of this Master Agreement will not be waived, altered, modified, supplemented, or amended in any manner whatsoever without prior written agreement of the Lead State and Contractor.
- II.3 Amendment Term.** The term of the Master Agreement may be amended past the initial term and stated renewal periods for a reasonable period if in the judgment of the Lead State a follow-on competitive procurement will be unavoidably delayed (despite good faith efforts) beyond the planned date of execution of the follow-on master agreement. This subsection will not be deemed to limit the authority of a Lead State under its state law to otherwise negotiate contract extensions.

III. Order of Precedence

- III.1 Order of Precedence.** The following Order of Precedence will apply to any purchase or Order made under this Master Agreement:
 - III.1.1** A Participating Entity's Participating Addendum ("PA");
 - III.1.2** The following Master Agreement Attachments: Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions, including A.1, A.2, and A.3 as applicable, Attachment B: Scope of Work, and Attachment C: Pricing Discounts and Schedule;
 - III.1.3** A Purchase Order, Service Level Agreement, or Statement of Work/specifications issued against the Master Agreement;
 - III.1.4** The Solicitation or, if separately executed after award, the Lead State's bilateral agreement that integrates applicable provisions;
 - III.1.5** Attachment D: Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State;
 - III.1.6** Attachment E: Contractor, Fulfillment Partner, or Third-party Provider's End User Agreement issued against a Participating Addendum. End User Agreements are expected to be negotiated by a Purchasing Entity seeking to utilize the solution at the time a Project is entered into;
 - III.1.7** Any other Attachments to the Master Agreement not listed above.
- III.2 Conflict.** These documents will be read to be consistent and complementary. Any conflict among these documents will be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.
- III.3 Participating Addenda.** Participating Addenda will not be construed to diminish, modify, or otherwise derogate any provisions in this Master Agreement between the Lead State and Contractor. The term of a Participating Addendum will not exceed the term of this Master Agreement, except when a Participating Entity determines an extension of its Participating Addendum is necessary to avoid a lapse in contract coverage and is permitted by law.

IV. Participants and Scope

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

Participating Entity and Contractor is executed.

- IV.2 Applicability of Master Agreement.** NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum, subject to Section III. For the purposes of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g., purchase order or contract) used by the Purchasing Entity to place the Order.
- IV.3 Scope of Work Updates.** At the discretion of the Lead State, and subject to agreement by the parties, the scope of this Master Agreement may be amended to include or accommodate new or updated models, versions, or technologies related to the objectives and deliverables set forth in the Solicitation.
- IV.4 Obligated Entities.** Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Participating Entities incur no financial obligations on behalf of other Purchasing Entities.
- IV.5 Notice of Participating Addendum.** Contractor shall email a fully executed PDF copy of each Participating Addendum to pa@naspovaluepoint.org to support documentation of participation and posting in appropriate databases.
- IV.6 Participating Entities.**
- IV.6.1** If not proscribed by law or by the Chief Procurement Official of the state in which the entity is located, an entity may be eligible to execute a Participating Addendum directly with Contractor. Such entities may include:
- IV.6.1.1** Political subdivisions, public agencies, and service districts;
- IV.6.1.2** Public and private educational institutions, including K-12 public, charter, and private schools; institutions of higher education; and trade schools;
- IV.6.1.3** Federally recognized tribes;
- IV.6.1.4** Quasi-governmental entities; and
- IV.6.1.5** Eligible non-profit organizations.
- IV.6.2** Prior to execution of a Participating Addendum with an entity listed above, Contractor shall coordinate with NASPO to confirm the entity's eligibility to execute a Participating Addendum. A determination that an entity is eligible to execute a Participating Addendum is not a determination that procurement authority exists; each entity must ensure it has the requisite procurement authority to execute a Participating Addendum.
- IV.7 Prohibition on Resale.** Subject to any specific conditions included in the

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

- IV.8 Individual Customers.** Except as may otherwise be agreed to by the Purchasing Entity and Contractor, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement and as the Participating Entity has in the Participating Addendum, including but not limited to any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.
- IV.9 Release of Information.** Throughout the duration of this Master Agreement, Contractor must secure from the Lead State prior approval for the release of information that pertains to the potential work or activities covered by the Master Agreement. This limitation does not preclude publication about the award of the Master Agreement or marketing activities consistent with any proposed and accepted marketing plan.
- IV.10 No Representations.** The Contractor shall not make any representations of NASPO ValuePoint, the Lead State, any Participating Entity, or any Purchasing Entity's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent.

V. NASPO ValuePoint Provisions

- V.1 Applicability.** NASPO ValuePoint is not a party to the Master Agreement. The terms set forth in Section V are for the benefit of NASPO ValuePoint as a third-party beneficiary of this Master Agreement.
- V.2 Administrative Fees**
 - V.2.1 NASPO ValuePoint Fee.** Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than sixty (60) days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee must be submitted quarterly and is based on all sales of Products and Services under the Master Agreement (less any charges for taxes or shipping). The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with a vendor's response to the Lead State's Solicitation.
 - V.2.2 State Imposed Fees.** Some states may require an additional fee be paid by Contractor directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee rate or amount, payment method, and schedule for such reports and payments will be incorporated into the applicable Participating Addendum. Unless agreed to in writing by the state, Contractor may not adjust the Master Agreement pricing to include the state fee for purchases made by Purchasing Entities

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

V.3 NASPO ValuePoint Summary and Detailed Usage Reports

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

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

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

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

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

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

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

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

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

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

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

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

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

V.5 NASPO ValuePoint eMarketPlace

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

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

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

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

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

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

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

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

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

- V.5.9** NASPO Participating Entities may have their own procurement system, separate from the NASPO eMarketPlace, that enables the use of certain NASPO Master Agreements. In the event one of these entities elects to use this NASPO ValuePoint Master Agreement (available through the eMarketPlace) but publish to their own eMarketPlace, Contractor agrees to work in good faith with the entity and NASPO to implement the catalog.
- V.5.10** In the event a Participating Entity has entity-specific catalog requirements set forth in its Participating Addendum (e.g., entity-specific pricing, restrictions in the scope of offerings, etc.), Contractor shall ensure its eMarketPlace Content for that Participating Entity accurately reflects and is compliant with these requirements.
- V.5.11** Implementation Timeline: Following the execution of Contractor's Master Agreement, NASPO will provide a written request to Contractor to begin the onboarding process into the eMarketPlace. Contractor shall have fifteen (15) days from receipt of written request to work with NASPO to set up an enablement schedule, at which time the technical documentation for onboarding shall be provided to Contractor. The schedule will include future calls and milestone dates related to test and go live dates.
 - V.5.11.1** Contractor's NASPO eMarketPlace account with eQuoting functionality shall minimally be established within thirty (30) days following the written request.
 - V.5.11.2** Contractor shall deliver either a (1) hosted catalog or (2) punchout site, pursuant to the mutually agreed upon enablement schedule.
 - V.5.11.3** NASPO will work with Contractor to decide which structures between hosted catalog, punchout site, and/or eQuoting as further described below will be provided by Contractor.
 - V.5.11.3.1** Hosted Catalog. By providing a hosted catalog, Contractor is providing a list of its awarded Products/Services and pricing in an electronic Data file in a format acceptable to NASPO, such as a tab delimited text file. Contractor is solely responsible for ensuring the most up-to-date versions of its Product/Service offerings approved by the Lead State under this Master Agreement are reflected in the eMarketPlace.
 - V.5.11.3.2** Punchout Site. By providing a punchout site, Contractor is providing its own online catalog, which must be capable of being integrated with the eMarketPlace as a Standard punchout via Commerce eXtensible Markup Language (cXML). Contractor shall validate that its online catalog is up-to-date. The site must also return detailed UNSPSC codes for each line item.
 - V.5.11.3.3** eQuoting. NASPO will work with Contractor to set up participation and use to provide eQuotes through the NASPO eMarketPlace. This requirement would be in addition to any requirement to provide a hosted catalog or punchout site.

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

- V.5.12.1** The most current pricing, including all applicable administrative fees and/or discounts, as well as the most up-to-date Product/Service offering the Contractor is authorized to provide in accordance with this Master Agreement;
- V.5.12.2** A Lead State contract identification number for this Master Agreement;
- V.5.12.3** Detailed Product line item descriptions;
- V.5.12.4** Pictures illustrating Products, services, or solutions where practicable; and
- V.5.12.5** Any additional NASPO, Lead State, or Participating Addendum requirements.

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

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

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

VI. Pricing, Payment & Leasing

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

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

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

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

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

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

VII. Ordering

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

VII.2 Quotes. Purchasing Entities may define entity-specific or project-specific requirements and informally compete the requirement among companies having a Master Agreement on an “as needed” basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to the Purchasing Entity’s rules and policies. The Purchasing Entity may in its sole discretion determine which Master Agreement Contractors should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost, and other factors considered.

VII.3 Applicable Rules. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities’ rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

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

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

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

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

VII.5.3 Financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

VII.5.4 Notwithstanding the expiration, cancellation or termination of this Master Agreement, Contractor shall perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration, cancellation, or termination of this Master Agreement, or in any manner inconsistent with this Master Agreement's terms.

VII.5.5 Orders for any separate indefinite quantity, task order, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

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

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

VII.6.1 The services or supplies being delivered;

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

VII.6.3 A billing address;

VII.6.4 Purchasing Entity contact information;

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

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

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

VII.7 Communication. All communications concerning administration of Orders placed must be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

VII.8 Contract Provisions for Orders Utilizing Federal Funds. Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this Master Agreement.

VIII. Shipping and Delivery

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

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

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

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

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

IX. Inspection and Acceptance

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

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

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

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

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

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

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

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

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

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

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

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

X. Warranty

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

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

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

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

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

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

XI. Product Title

- XI.1 Conveyance of Title.** If both the Contractor and Purchasing Entity intend for any Products or Services being purchased to be owned by the Purchasing Entity after the sale (as opposed to a subscription service, service term, or other right of use), upon acceptance by the Purchasing Entity, Contractor shall convey to Purchasing Entity title to the Product free and clear of all liens, encumbrances, or other security interests.
- XI.2 Embedded Software.** Transfer of title to the Product must include an irrevocable and perpetual license to use any Embedded Software in the Product. If Purchasing Entity subsequently transfers title of the Product to another entity, Purchasing Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title. A subsequent transfer of this software license will be at no additional cost or charge to either Purchasing Entity or Purchasing Entity's transferee.
- XI.3 License of Pre-Existing Intellectual Property.** Contractor grants to the Purchasing Entity a nonexclusive, perpetual, royalty-free, irrevocable, license to use, publish, translate, reproduce, transfer with any sale of tangible media or Product, perform, display, and dispose of the Intellectual Property, and its derivatives, used or delivered under this Master Agreement, but not created under it ("Pre-existing Intellectual Property"). The Contractor shall be responsible for ensuring that this license is consistent with any third-party rights in the Pre-existing Intellectual Property.

XII. Indemnification

- XII.1 General Indemnification.** The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers and employees, from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property arising from any act, error, or omission of the Contractor, its employees or Subcontractors or volunteers, at any tier, relating to performance under this Master Agreement.
- XII.2 Intellectual Property Indemnification.** The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers and employees ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use infringes Intellectual Property rights of another person or entity ("Intellectual Property Claim").
- XII.2.1** The Contractor's obligations under this section will not extend to any combination of the Product with any other product, system or method, unless the Product, system or method is:
- XII.2.1.1** provided by the Contractor or the Contractor's subsidiaries or affiliates;
 - XII.2.1.2** specified by the Contractor to work with the Product;
 - XII.2.1.3** reasonably required to use the Product in its intended manner, and the infringement could not have been avoided

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

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

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

XII.2.3 The Indemnified Party shall furnish, at the Contractor’s reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of the Intellectual Property Claim and the Contractor shall be liable for all costs and expenses, including reasonable attorneys’ fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim.

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

XIII. Insurance

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

XIII.2 Class. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity’s State and having a rating of A-, Class VII or better, in the most recently published edition of A.M. Best’s Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement’s termination or, at a Participating Entity’s option, result in termination of its Participating Addendum.

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

XIII.3.1 Contractor shall maintain Commercial General Liability insurance covering premises operations, independent contractors, Products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than \$1 million per occurrence and \$2 million general aggregate;

XIII.3.2 CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

- XIII.4 Notice of Cancellation.** Contractor shall pay premiums on all insurance policies. Contractor shall provide notice to a Participating Entity who is a state within five (5) business days after Contractor is first aware of expiration, cancellation or nonrenewal of such policy or is first aware that cancellation is threatened or expiration, nonrenewal or expiration otherwise may occur.
- XIII.5 Notice of Endorsement.** Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) provides that written notice of cancellation will be delivered in accordance with the policy provisions, and (2) provides that the Contractor's liability insurance policy will be primary, with any liability insurance of any Participating State as secondary and noncontributory.
- XIII.6 Participating Entities.** Contractor shall provide to Participating States and Participating Entities the same insurance obligations and documentation as those specified in Section XIII, except the endorsement is provided to the applicable Participating State or Participating Entity.
- XIII.7 Furnishing of Certificates.** Contractor shall furnish to the Lead State copies of certificates of all required insurance in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement and prior to performing any work. Copies of renewal certificates of all required insurance will be furnished within thirty (30) days after any renewal date to the applicable state Participating Entity. The Lead State or a Participating Entity may request proof of insurance and copies of certificates of insurance at any time during the term of the Master Agreement. Failure to provide evidence of coverage may, at the sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.
- XIII.8 Disclaimer.** Insurance coverage and limits will not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

XIV. General Provisions

XIV.1 Records Administration and Audit

- XIV.1.1** The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and Orders placed by Purchasing Entities under it to the extent and in such detail as will adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or Orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right will survive for a

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

XIV.1.2 Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or Orders or underpayment of fees found as a result of the examination of the Contractor's records.

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

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

XIV.2.1 Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity or Purchasing Entity's clients.

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

XIV.2.1.2 Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information.

XIV.2.1.3 Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity; or (6) is independently developed by employees, agents or Subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

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

Master Agreement.

- XIV.2.2.1** Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information.
- XIV.2.2.2** Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person.
- XIV.2.2.3** Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information.
- XIV.2.2.4** Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits, and evidence of the performance of this Master Agreement.
- XIV.2.3 Injunctive Relief.** Contractor acknowledges that Contractor's breach of Section 14.2 would cause irreparable injury to the Purchasing Entity that cannot be adequately compensated in monetary damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.
- XIV.2.4 Purchasing Entity Law.** These provisions will be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.
- XIV.2.5 NASPO ValuePoint.** The rights granted to Purchasing Entities and Contractor's obligations under this section will also extend to NASPO ValuePoint's Confidential Information, including but not limited to Participating Addenda, Orders or transaction Data relating to Orders under this Master Agreement that identify the entity/customer, Order dates, line-item descriptions and volumes, and prices/rates. This provision does not apply to disclosure to the Lead State, a Participating State, or any governmental entity exercising an audit, inspection, or examination pursuant to this Master Agreement. To the extent permitted by law,

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

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

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

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

XIV.3 Assignment/Subcontracts

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

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

XIV.4 Changes in Contractor Representation. The Contractor must, within ten (10) calendar days, notify the Lead State in writing of any changes in the Contractor's key administrative personnel managing the Master Agreement. The Lead State reserves the right to approve or reject changes in key personnel, as identified in the Contractor's proposal. The Contractor shall propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

XIV.5 Independent Contractor. Contractor is an independent Contractor. Contractor has no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and shall not hold itself out as agent except as expressly set forth herein or as expressly set forth in an applicable Participating Addendum or Order.

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

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

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

XIV.8 Defaults and Remedies

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

XIV.8.1.1 Nonperformance of contractual requirements;

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

XIV.8.1.3 Any certification, representation or warranty by Contractor in response to the Solicitation or in this Master Agreement that proves to be untrue or materially misleading;

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

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

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

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

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

XIV.8.3.1 Any remedy provided by law;

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

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

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

XIV.8.3.5 Suspension of Contractor's performance; and

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

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

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

XIV.10 Debarment. The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in public procurement or contracting by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

XIV.11 No Waiver of Sovereign Immunity

XIV.11.1 In no event will this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from

any claim or from the jurisdiction of any court.

XIV.11.2 This section applies to a claim brought against the Participating Entities who are states only to the extent Congress has appropriately abrogated the state's sovereign immunity and is not consent by the state to be sued in federal court. This section is also not a waiver by the state of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

XIV.12 Governing Law and Venue

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

XIV.12.2 Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the state serving as Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement will be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum will be in the Purchasing Entity's state.

XIV.12.3 If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing Order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; a Participating State if a named party; the state where the Participating Entity or Purchasing Entity is located if either is a named party.

XIV.13 Assignment of Antitrust Rights. Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's State antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided in that state for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at the Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

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

Attachment A.1 – Software Publisher Terms and Conditions

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

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

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

1. Definitions:

- a. **Authorized Persons:** The service provider's employees, contractors, Subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.
- b. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. .
- c. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.
- d. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.
- e. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notifications.
- f. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.
- g. **Service provider:** The Contractor and its employees, Subcontractors, agents and affiliates who are providing the services agreed to under the contract. Service provider also includes a Third-party Provider providing services under the contract.
- h. **Software-as-a-Service (SaaS):** The capability provided to the consumer to use the

provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure — including network, servers, operating systems, storage or even individual application capabilities — with the possible exception of limited user-specific application configuration settings.

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

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

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

- a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with NIST SP 800- 53 (then current, or prior version compliant with the appropriate certification body's requirements) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
- b. All data obtained by the service provider in the performance of this contract shall become and remain property of the public jurisdiction.
- c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). Unless otherwise stipulated, the service provider is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the SLA, End User Agreement, or otherwise made a part of this contract.
- d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and

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

- e. At no time shall any data or processes that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- f. The service provider shall not use any information collected in connection with the service issued from this contract for any purpose other than fulfilling the service.

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

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

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

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

- a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800- 53 (then current, or prior version compliant with the appropriate certification body's requirements) Access Controls.
- b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the Purchasing Entity for follow the sun technical support.
- c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will

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

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

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

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

- a. **Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the public jurisdiction should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.
- b. **Security Incident Reporting Requirements:** The service provider shall report a security incident to the appropriate public jurisdiction identified contact within the manner and timeframe defined in law, a Participating Addendum, or End User Agreement.
- c. **Breach Reporting Requirements:** If the service provider has actual knowledge of a confirmed data breach that affects the security of any public jurisdiction content that is subject to applicable data breach notification law, the service provider shall notify the appropriate public jurisdiction identified contact within 48 hours or sooner — unless shorter time is required by applicable law — and take commercially reasonable measures to address the data breach in a timely manner.

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

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

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

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

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

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

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

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

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

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

14. Access to Security Logs and Reports:

- a. The service provider shall provide reports to the public jurisdiction in a format specified in the SLA or End User Agreement. Reports shall include latency statistics, date and time stamps, user access IP addresses, source and destination IP addresses, system events (e.g., failed and successful events — system shutdown or starting a service, errors, anomalous/abnormal activity or system events, etc.), log-on/authentication attempts (failed and successful), user access history, account changes (e.g., account creation and deletion, account privilege assignment, etc.), security policy changes, system configuration changes, usage information (e.g., number of transactions occurring in a certain period of time) and transaction size (e.g., email message size, file transfer size, etc.), and security logs for all public jurisdiction data related to this contract.
- b. The service provider and the public jurisdiction share security responsibilities. The service provider is responsible for providing a secure infrastructure (e.g., storage and servers), virtualization/ hypervisor, operating system, middleware and runtime, applications and networking. The service provider and the public jurisdiction typically share responsibility for identity, credential and access management; networking; and data. The methods and conditions for authorized access to logs/reports and the format for the logs/reports shall be specified and agreed upon by both parties in the SLA or End User Agreement. Specific shared responsibilities are identified in the SLA or End User Agreement.

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

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

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

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

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

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

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

20. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA or End User Agreement.

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

22. Subcontractor Disclosure: The service provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all Subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who shall be involved in any application development and/or operations.

23. Business Continuity and Disaster Recovery:

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

24. Compliance with Accessibility Standards:

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

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

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

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

28. Termination and Suspension of Service:

- a. In the event of a contract termination, the service provider shall return public jurisdiction's data in a CSV or other mutually agreeable format at a time agreed to by the parties. The service provider also will provide for the subsequent secure disposal of public jurisdiction data.
- b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction data.
- c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of:
 1. 10 days after the effective date of termination, if the termination is in accordance with the contract period
 2. 30 days after the effective date of termination, if the termination is for convenience
 3. 60 days after the effective date of termination, if the termination is for cause

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

- d. The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established in the SOW.
- e. The service provider shall securely dispose of all requested data in all forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data

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

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

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

1. Definitions:

- a. **Authorized Persons:** The service provider's employees, contractors, Subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.
- b. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- c. **Platform-as-a-Service (PaaS):** The capability provided to the consumer to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations..
- d. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.
- e. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.
- f. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.
- g. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.
- h. **Service Provider:** The Contractor and its employees, Subcontractors, agents and affiliates who are providing the services agreed to under the contract. Service provider also includes a Third-party Provider providing services under the contract.
- i. **Statement of Work:** A Statement of Work (SOW) is a detailed document issued against the Master Agreement that defines the scope, deliverables, timelines, responsibilities,

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

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

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

- a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
- b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction.
- c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). The SLA or End User Agreement and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the Statement of Work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.
- d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.
- e. At no time shall any data or processes which either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are the responsibility of the service provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime) and provide service to customers as defined in the SLA or End User Agreement.

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

22. Sub-Contractor Disclosure: The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all Subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider, and who will be involved in any application development and/or operations.

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

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

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

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

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

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

28. Termination and Suspension of Service:

- a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.
- b. During any period of service suspension, the service provider shall not intentionally erase any public jurisdiction digital content.
- c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content.
- d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/ DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

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

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

1. Definitions:

- a. **Authorized Persons:** The service provider's employees, contractors, Subcontractors or other agents who need to access the public jurisdiction's personal data to enable the service provider to perform the services required.
- b. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- c. **d. Infrastructure-as-a-Service (IaaS):** The capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls). .
- d. **Public Jurisdiction:** Any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.
- e. **Public Jurisdiction Data:** All data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.
- f. **Public Jurisdiction Identified Contact:** The person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.
- g. **Security Incident:** The potentially unauthorized access by non-authorized persons to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non- public data within the possession or control of the service provider. A security incident may or may not turn into a data breach. .
- h. **Service Provider:** The Contractor and its employees, Subcontractors, agents and affiliates who are providing the services agreed to under the contract. Service provider also includes a Third-party Provider providing services under the contract.

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

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

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

- a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data within its control. Such security measures shall be in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.
- b. All data obtained by the service provider within its control in the performance of this contract shall become and remain property of the public jurisdiction.
- c. Unless otherwise stipulated, all personal data and non-public data shall be encrypted at rest and in transit with controlled access in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements). The SLA or End User Agreement and contract document will specify which party is responsible for encryption and access control of the public jurisdiction data for the service model under contract. If the statement of work and the contract are silent, then the public jurisdiction is responsible for encryption and access control.
- d. Unless otherwise stipulated, it is the public jurisdiction's responsibility to identify data it deems as non-public data to the service provider. The level of protection and encryption for all non-public data shall be identified and made a part of this contract. At no time shall any data or processes which either belong to or are intended for the use of public jurisdiction or its officers, agents or employees be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

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

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

requirements) Privacy Controls.

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

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

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

- a. Providing a multifactor authentication access mechanism for all its personnel and contractors to access any system and data management tool which acts upon any public jurisdiction data in accordance with NIST SP 800-53 (then current, or prior version compliant with the appropriate certification body's requirements) Access Controls.
- b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the Purchasing Entity for follow the sun.
- c. Maintaining government data and allowing the downloading of that data for a minimum period of 90 days after the termination of the agreement between the public jurisdiction and the service provider. After this period, the service provider will destroy/delete the data and all copies wherever they may reside and provide a certificate of destruction/deletion to the public jurisdiction.

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

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

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

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

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

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

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

- a. The service provider, unless stipulated otherwise, shall immediately notify the appropriate public jurisdiction identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
- b. The service provider, unless stipulated otherwise, shall notify the appropriate public jurisdiction identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a data breach. The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document actions taken in response to the data breach, including any post-incident review of events and changes in business practices.
- c. Unless otherwise stipulated, if a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifying individuals, regulators or others required by state law; (3) providing a credit monitoring service required by state or federal law; (4) providing a website or a toll-free number and call center for affected individuals required by state law; and (5) completing all corrective actions as reasonably determined by the service provider based on root cause. These costs shall not exceed the average per-record, per-person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach. All actions [1 through 5] are subject to this contract's limitation of liability.

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

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

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

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

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

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

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

14. Access to Security Logs and Reports:

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

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

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

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

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

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

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

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

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

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

Review of control documentation by internal staff or 3PAOs

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

20. Responsibilities and Uptime Guarantee: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are the responsibility of the service provider. The system shall be available 24/7/365, with agreed-upon maintenance downtime, and provide service to customers as defined in the SLA or End User Agreement.

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

22. Subcontractor Disclosure: The service provider shall identify all strategic business partners related to services provided under this contract, including but not limited to all Subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the service provider and who shall be involved in any application development and/or operations.

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

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

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

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

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

28. Termination and Suspension of Service:

- a. In the event of an early contract termination, the service provider shall allow the public jurisdiction to retrieve its digital content and provide for the subsequent secure disposal of public jurisdiction digital content.
- b. During any period of suspension, the service provider shall not intentionally erase any public jurisdiction digital content.
- c. If any services are terminated or the entire agreement is terminated, the service provider shall not intentionally erase any public jurisdiction data for a period of 45 days after the effective date of a termination for convenience, or 60 days after the effective date of a termination for cause. After such period, the service provider has no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control. In the event of a termination for cause, the service provider will impose no fees the customer for access and retrieval of digital content.
- d. After termination of the contract and the prescribed retention period, the provider shall securely dispose of all digital content in all forms, such as disk, CD/ DVD, backup tape and paper. The public jurisdiction's digital content shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

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

Attachment A.2 – On-Premises Terms and Conditions

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

Attachment B SCOPE OF WORK

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

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

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

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

I. Scope of Work Overview:

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

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

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

Definitions:

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

1. Definitions, Roles, and Responsibilities:

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

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

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

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

Fulfillment Partner: Is an agent authorized to act on behalf of a Contractor including a Contractor who is either a Direct Service Provider or Value-added Reseller. Fulfillment Partners may act as an authorized reseller, implementer, service provider, or other related role to fulfill and complete the delivery and performance of a Product or solution that is being purchased through a Master Agreement. Fulfillment Partners may quote, invoice, and receive payment on behalf of a Contractor. To add a Fulfillment Partner to a Master Agreement, the Contractor must submit a request to the Lead State for approval providing the Fulfillment Partner’s vendor information, W-9, and updated list of Fulfillment Partners containing their contact information, which states/areas they are authorized to act in, and other pertinent information related to the products, services, solutions, etc. 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)	2%	2%	2%	2%	2%
Value-Added Resellers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	2%	2%	2%	2%	2%
Maximum Markup %	Software (Saas)	Infrastructure (IaaS)	Platform (PaaS)	On-Premises	Value Added Services*
Value-Added Resellers: Maximum Markup %	95%	95%	95%	95%	95%

Attachment D

Contractor's Response to the Solicitation

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

Attachment E

End User Agreements

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

Attachment F: Third-party Provider Agreement (Template)

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

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

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

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

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

Lead State Approval: