All using Agencies of the Commonwealth, Participating Political Subdivision, Authorities, Private Colleges and Universities

FULLY EXECUTED
Contract Number: 4400034320
Original Contract Effective Date: 09/03/2026
Valid From: 09/16/2026 To: 09/15/2031

Your SAP Vendor Number with us: 316904

Purchasing Agent
Name: Cropper Scott
Phone: 717-346-3819
Fax:

Supplier Name/Address:
CARAHSOFT TECHNOLOGY CORP
11493 SUNSET HILLS RD
RESTON VA 20190-5230 US

Supplier Phone Number: 703-871-8500
Supplier Fax Number: 703-871-8505

Please Deliver To:

To be determined at
the time of the Purchase Order
unless specified below.

Contract Name:
Carahsoft Cloud and Software Solutions

Payment Terms
NET 30

Solicitation No.: Issuance Date:

Supplier Bid or Proposal No. (if applicable): Solicitation Submission Date:

This contract is comprised of: The above referenced Solicitation, the Supplier's Bid or Proposal, and any documents attached to this Contract or incorporated by reference.

Item	Material/Service Desc	Qty	UOM	Price	Per Unit	Total
1	Software, Licensing and Renewals	0.000		0.00	1	0.00
2	Software Maintenance and Support	0.000		0.00	1	0.00
3	Professional Services	0.000		0.00	1	0.00
4	Hardware as part of integrated IT Servic	0.000		0.00	1	0.00

General Requirements for all Items:

Information:

Supplier's Signature ______________________

Printed Name ______________________

Title ______________________

Date ______________________

FULLY EXECUTED

Contract Number: 4400034320

Original Contract Effective Date: 09/03/2026

Valid From: 09/16/2026 To: 09/15/2031

Supplier Name:

CARAHSOFT TECHNOLOGY CORP

Header Text

This Participating Addendum ("Addendum") is entered into pursuant to the State of Utah Cooperative Contract, Contract Number LS4983 (“Utah Cooperative Contract”), between Carahsoft Technology Corp. (“Contractor”) and the State of Utah Division of Purchasing ("Utah"). The parties to this Addendum hereby create a separate contract between the Contractor and the Commonwealth of Pennsylvania (“Commonwealth”) acting through its Department of General Services ("DGS").

Utah, pursuant to law governing federal acquisitions, entered into the Utah Cooperative Contract with the Contractor, pursuant to which the Contractor provides various On-Premise and Cloud products and related services, including Software as a Service (SaaS), Infrastructure as Service (IaaS), and Platforms as a Service (PaaS), and related Services as described in the Utah Cooperative Contract.

No further information for this Contract

Information:

IT CONTRACT TERMS AND CONDITIONS

1. DEFINITIONS.

(a) Agency. The department, board, commission or other agency of the Commonwealth of Pennsylvania listed as the Purchasing Agency. If a COSTARS entity or external procurement activity has issued an order against this Contract, that entity shall also be identified as "Agency."

(b) Commonwealth. The Commonwealth of Pennsylvania.

(c) Contract. The integrated documents as defined in **Section 11, Order of Precedence**.

(d) Contracting Officer. The person authorized to administer this Contract for the Commonwealth and to make written determinations with respect to the Contract.

(e) Data. Any recorded information, regardless of the form, the media on which it is recorded or the method of recording.

(f) Days. Calendar days, unless specifically indicated otherwise.

(g) Developed Works. All of the fully or partially complete property, whether tangible or intangible prepared by the Contractor for ownership by the Commonwealth in fulfillment of the requirements of this Contract, including but not limited to: documents; sketches; drawings; designs; works; papers; files; reports; computer programs; documentation; data; records; software; samples; literary works and other works of authorship. Developed Works include all material necessary to exercise all attributes of ownership or of the license granted in **Section 46, Ownership of Developed** Works but shall not include any underlying source code or proprietary Contractor or third-party Software, Supplies, or Services which are properly represented to the Commonwealth as such.

(h) Documentation. All materials required to support and convey information about the Services or Supplies required by this Contract, including, but not limited to: written reports and analyses; diagrams maps, logical and physical designs; system designs; computer programs; flow charts; and disks and/or other machine-readable storage media.

(i) Expiration Date. The last valid date of the Contract, as indicated in the Contract documents to which these IT Contract Terms and Conditions are attached.

(j) Metadata. (i) Any Data that is created from Commonwealth or Agency Data which results in an anonymized output that does not identify the Commonwealth, the Agency, or its individual Data in any manner, and (ii) product usage data, diagnostics data, and performance information that the Contractor collects or otherwise generates from the Commonwealth or Agency's use of the Services. These outputs are generated only for lawful business purposes such as product/service improvement, training, developing algorithms for machine learning, industry benchmarking, and analytics.

(k) Purchase Order. Written authorization for Contractor to proceed to furnish Supplies or Services.

(l) Proposal. Contractor's response to a Solicitation issued by the Issuing Agency, as accepted by the Commonwealth.

(m) Services. All Contractor activity necessary to satisfy the Contract.

(n) Software. A collection of one or more programs, databases or microprograms fixed in any tangible medium of expression that comprises a sequence of instructions (source code) to carry out a process in, or convertible into, a form executable by an electronic computer (object code).

(o) Solicitation. A document issued by the Commonwealth to procure Services or Supplies, e.g., Request for Proposal; Request for Quotation; Supplier Pricing Request; or Invitation for Bid, including all attachments and addenda thereto.

(p) Supplies. All tangible and intangible property including, but not limited to, materials and equipment provided by the Contractor to satisfy the Contract.

2. TERM OF CONTRACT.

(a) Term. The term of the Contract shall commence on the Effective Date and shall end on the Expiration Date identified in the Contract, subject to the other provisions of the Contract.

(b) Effective Date. The Effective Date shall be one of the following:

(i) the date the Contract has been fully executed by the Contractor and all approvals required by Commonwealth contracting procedures have been obtained; or

(ii) the date stated in the Contract, whichever is later.

3. COMMENCEMENT OF PERFORMANCE.

(a) General. The Contractor shall not commence performance and the Commonwealth shall not be liable to pay the Contractor for any supply furnished or work performed or expenses incurred, until both of the following have occurred:

(i) the Effective Date has occurred; and

(ii) the Contractor has received a Purchase Order or other written notice to proceed signed by the Contracting Officer.

(b) Prohibition Prior to Effective Date. No Commonwealth employee has the authority to verbally direct the commencement of any Service or delivery of any Supply under this Contract prior to the date performance may commence. The Contractor hereby waives any claim or cause of action for any Service performed or Supply delivered prior to the date performance may commence. In the event that the Contractor is directed otherwise by the Commonwealth, the Contractor may submit a proposal to the Commonwealth for settlement of any additional expenses incurred due to such direction. The Commonwealth shall review and discuss the proposal with the Contractor in good faith.

4. EXTENSION OF CONTRACT TERM.

The Commonwealth reserves the right, upon notice to the Contractor, to extend the term of the Contract for up to **three months** upon the same terms and conditions.

5. ELECTRONIC SIGNATURES.

(a) The Contract and/or Purchase Orders may be electronically signed by the Commonwealth.

(i) *Contract*. "Fully Executed" at the top of the first page of the Contract output indicates that the signatures of all the individuals required to bind the Commonwealth to the terms of the Contract have been obtained. If the Contract output form does not have "Fully Executed" at the top of the first page, the Contract has not been fully executed.

(ii) *Purchase Orders*. The electronically-printed name of the Purchasing Agent on the Purchase Order indicates that all approvals required by Commonwealth contracting procedures have been obtained.

(b) The Commonwealth and the Contractor specifically agree as follows:

(i) *Written signature not required.* No handwritten signature shall be required in order for the Contract or Purchase Order to be legally enforceable.

(ii) *Validity; admissibility*. The parties agree that no writing shall be required in order to make the Contract or Purchase Order legally binding, notwithstanding contrary requirements in any law or regulation. The parties hereby agree not to contest the validity or enforceability of the Contract executed electronically, or acknowledgement issued electronically, under the provisions of a statute of frauds or any other applicable law relating to whether certain agreements be in writing and signed by the party bound thereby. Any genuine Contract or acknowledgement executed or issued electronically, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings, will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form. Neither party shall contest the admissibility of copies of a genuine Contract or acknowledgements under either the business records exception to the hearsay rule or the best evidence rule on the basis that the Contract or acknowledgement were not in writing or signed by the parties. A Contract or acknowledgment shall be deemed to be genuine for all purposes if it is transmitted to the location designated for such documents.

(c) Verification. Each party will immediately take steps to verify any document that appears to be obviously garbled in transmission or improperly formatted to include re-transmission of any such document if necessary.

6. PURCHASE ORDERS.

(a) Purchase Orders. The Commonwealth may issue Purchase Orders against the Contract or issue a Purchase Order as the Contract. These Purchase Orders constitute the Contractor’s authority to make delivery. All Purchase Orders received by the Contractor up to, and including, the Expiration Date of the Contract are acceptable and must be performed in accordance with the Contract. Each Purchase Order will be deemed to incorporate the terms and conditions set forth in the Contract.

(b) Electronic transmission. Purchase Orders may be issued electronically or through facsimile equipment. The electronic transmission of a Purchase Order shall require acknowledgement of receipt of the transmission by the Contractor.

(c) Receipt. Receipt of the electronic or facsimile transmission of the Purchase Order shall constitute receipt of a Purchase Order.

(d) Received next business day. Purchase Orders received by the Contractor after 4 p.m. will be considered received the following business day.

(e) Commonwealth Purchasing Card. Purchase Orders under $10,000 in total amount may also be made in person or by telephone using a Commonwealth Purchasing Card. When an order is placed by telephone, the Commonwealth agency shall provide the agency name, employee name, credit card number and expiration date of the card. The Contractor agrees to accept payment through the use of a Commonwealth Purchasing card.

7. CONTRACT SCOPE.

The Contractor agrees to furnish the requested Services and Supplies to the Commonwealth as such Services and Supplies are defined in this Contract.

8. ACCESS TO COMMONWEALTH FACILITIES.

If the Contractor must perform work at a Commonwealth facility outside of the daily operational hours set forth by the Commonwealth, it must make arrangements with the Commonwealth to assure access to the facility and equipment. No additional payment will be made on the basis of lack of access.

9. NON-EXCLUSIVE CONTRACT.

The Commonwealth reserves the right to purchase Services and Supplies within the scope of this Contract through other procurement methods whenever the Commonwealth deems it to be in its best interest.

10. INFORMATION TECHNOLOGY POLICIES.

Reserved

11. ORDER OF PRECEDENCE.

If any conflicts or discrepancies should arise in the terms and conditions of this Contract, or the interpretation thereof, the order of precedence shall be:

(a) The documents containing the parties' signatures;

(b) The IT Contract Terms and Conditions;

(c) The Solicitation; and

(d) The Proposal.

12. CONTRACT INTEGRATION.

(a) Final contract. This Contract constitutes the final, complete, and exclusive Contract between the parties, containing all the terms and conditions agreed to by the parties.

(b) Prior representations. All representations, understandings, promises, and agreements pertaining to the subject matter of this Contract made prior to or at the time this Contract is executed are superseded by this Contract.

(c) Conditions precedent. There are no conditions precedent to the performance of this Contract except as expressly set forth herein.

(d) Sole applicable terms. No contract terms or conditions are applicable to this Contract except as they are expressly set forth herein.

(e) Other terms unenforceable. The Contractor may not require the Commonwealth or any user of the Services or Supplies acquired within the scope of this Contract to sign, click through, or in any other way agree to any terms associated with use of or interaction with those Services and/or Supplies, unless the Commonwealth has approved the terms in writing in advance under this Contract, and the terms are consistent with this Contract and Sec. 7 of the Addendum. Further, changes to terms may be accomplished only by processes set out in this Contract; no quotations, invoices, business forms or other documentation, or terms referred to therein, shall become part of this Contract merely by their submission to the Commonwealth or their ordinary use in meeting the requirements of this Contract. Any terms imposed upon the Commonwealth or a user in contravention of this subsection (e) must be removed at the direction of the Commonwealth and shall not be enforced or enforceable against the Commonwealth or the user.

13. PERIOD OF PERFORMANCE.

The Contractor, for the term of this Contract, shall complete all Services and provide all Supplies as specified under the terms of this Contract. In no event shall the Commonwealth be responsible or liable to pay for any Services or Supplies provided by the Contractor prior to the Effective Date, and the Contractor hereby waives any claim or cause of action for any such Services or Supplies.

14. INDEPENDENT PRIME CONTRACTOR.

(a) Independent contractor. In performing its obligations under the Contract, the Contractor will act as an independent contractor and not as an employee or agent of the Commonwealth.

(b) Sole point of contact. The Contractor will be responsible for all Services and Supplies in this Contract whether or not Contractor provides them directly. Further, the Contractor is the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

15. SUBCONTRACTS.

The Contractor may subcontract any portion of the Services or Supplies described in this Contract to third parties selected by Contractor and approved in writing by the Commonwealth, whose approval shall not be unreasonably withheld. Notwithstanding the above, if Contractor has disclosed the identity of subcontractor(s) together with the scope of work to be subcontracted in its Proposal, award of the Contract is deemed approval of all named subcontractors and a separate approval is not required. The existence of any subcontract shall not change the obligations of Contractor to the Commonwealth under this Contract. The Commonwealth reserves the right, for good cause, to require that the

Contractor remove a subcontractor from the project. The Commonwealth will not be responsible for any costs incurred by the Contractor in replacing the subcontractor if good cause exists.

16. OTHER CONTRACTORS.

The Commonwealth may undertake or award other contracts for additional or related work, and the Contractor shall fully cooperate with other contractors and Commonwealth employees and coordinate its Services and/or its provision of Supplies with such additional work as may be required. The Contractor shall not commit or permit any act that will interfere with the performance of work by any other contractor or by Commonwealth employees. This section shall be included in the Contracts of all contractors with which this Contractor will be required to cooperate. The Commonwealth shall equitably enforce this section as to all contractors to prevent the imposition of unreasonable burdens on any contractor.

17. ENHANCED MINIMUM WAGE.

(a) Enhanced Minimum Wage. Contractor shall pay no less than $15.00 per hour to its employees for all hours worked directly performing the services called for in this contract/lease, and for an employee's hours performing ancillary services necessary for the performance of the services or lease when the employee spends at least 20% of their time performing ancillary services in a given work week.

(b) Adjustment. Beginning July 1, 2023, and annually thereafter, the minimum wage rate will be increased by an annual cost-of-living adjustment using the percentage change in the Consumer Price Index for All Urban Consumers (CPI-U) for Pennsylvania, New Jersey, Delaware, and Maryland. The Commonwealth will publish applicable adjusted amount in the Pennsylvania Bulletin by March 1 of each year to be effective the following July 1.

(c) Exceptions. These Enhanced Minimum Wage Provisions do not apply to employees

(i) Exempt from minimum wage under the Minimum Wage Act of 1968;

(ii) covered by a collective bargaining agreement;

(iii) required to be paid a higher wage under another state or federal law governing the services, including the Prevailing Wage Act and Davis-Bacon Act; or

(iv) required to be paid a higher wage under any state or local policy or ordinance.

(d) Notice. The Contractor shall: (1) post this Enhanced Minimum Wage Provision for the entire period of the contract conspicuously in easily-accessible and well-lighted places customarily frequented by employees at or near where the contracted services are performed; or (2) for the entire period of the contract, provide electronic notice of this clause to its employees not less than annually.

(e) Records. Contractor must maintain and, upon request and within the time periods requested by the Commonwealth, provide to the Commonwealth all employment and wage records necessary to document compliance with these Enhanced Minimum Wage Provisions.

(f) Sanctions. Contractor's failure to comply with these Enhanced Minimum Wage Provisions may result in the imposition of sanctions, which may include, but are not limited to, termination of the contract or lease, nonpayment, debarment, or referral to the Office of General Counsel for appropriate civil or criminal referral.

(g) Subcontractors. The Contractor shall include the requirements of these Enhanced Minimum Wage Provisions in its subcontracts under this contact or lease to ensure that these requirements are binding on its subcontractors.

18. COMPENSATION.

(a) General. The Contractor shall be required to perform at the price(s) quoted in the Contract. All items shall be performed within the time period(s) specified in the Contract. The Contractor shall be compensated only for items supplied and Services performed to the satisfaction of the Commonwealth.

(b) Travel. The Contractor shall not be allowed or paid travel or per diem expenses except as specifically set forth in the Contract. If not otherwise specified in the Contract, travel and related expenses shall be reimbursed in accordance with Management Directive 230.10 Amended, *Commonwealth Travel Policy*, and Manual 230.1, *Commonwealth Travel Procedures Manual*.

19. BILLING REQUIREMENTS.

(a) Unless the Contractor has been authorized by the Commonwealth for Evaluated Receipt Settlement or Vendor Self-Invoicing, the Contractor shall include in all of its invoices the following minimum information:

(i) Vendor name and "Remit to" address, including SAP Vendor number;

(ii) Bank routing information, if ACH;

(iii) SAP Purchase Order number;

(iv) Delivery Address, including name of Commonwealth agency;

(v) Description of the supplies/services delivered in accordance with SAP Purchase Order (include Purchase Order line number if possible);

(vi) Quantity provided;

(vii) Unit price;

(viii) Price extension;

(ix) Total price; and

(x) Delivery date of supplies or services.

(b) If an invoice does not contain the minimum information set forth in this section, and comply with the provisions located at https://www.budget.pa.gov/Programs/Pages/E-Invoicing.aspx, relating to the Commonwealth E-Invoicing Program, the Commonwealth may return the invoice as improper. If the Commonwealth returns an invoice as improper, the time for processing a payment will be suspended until the Commonwealth receives a correct invoice. The Contractor may not receive payment until the Commonwealth has received a correct invoice.

20. PAYMENT.

(a) Payment Date. The Commonwealth shall put for reasonable efforts to make payment by the required payment date. The required payment date is:

(i) the date on which payment is due under the terms of the Contract;

(ii) **30 days** after a proper invoice actually is received at the "Bill To" address if a date on which payment is due is not specified in the Contract (a "proper" invoice is not received until the Commonwealth accepts the service as satisfactorily performed); or

(iii) the payment date specified on the invoice if later than the dates established by paragraphs (a)(i) and (a)(ii), above.

(b) Delay; Interest. Payment may be delayed if the payment amount on an invoice is not based upon the price(s) as stated in the Contract. If any payment is not made within **15 days** after the required payment date, the Commonwealth may pay interest as determined by the Secretary of Budget in accordance with Act of December 13, 1982, P.L. 1155, No. 266, 72 P. S. § 1507, (relating to interest penalties on Commonwealth accounts) and accompanying regulations 4 Pa. Code §§ 2.31—2.40 (relating to interest penalties for late payments to qualified small business concerns).

(c) Payment should not be construed by the Contractor as acceptance of the Service performed by the Contractor. The Commonwealth reserves the right to conduct further testing and inspection after payment, but within ten business days after performance, and to reject the service if such post payment testing or inspection discloses a defect or a failure to meet specifications.

21. AUTOMATED CLEARING HOUSE (ACH) PAYMENTS.

(a) Payment Method. The Commonwealth shall make contract payments through the Automated Clearing House (ACH). Within ten days of award of the contract or purchase order, the Contractor must submit or must have submitted its ACH information within its user profile in the Commonwealth's procurement system (SRM).

(b) Unique Identifier. The Contractor must submit a unique invoice number with each invoice submitted. The Commonwealth shall list the Contractor's unique invoice number on its ACH remittance advice to enable the Contractor to properly apply the state agency's payment to the invoice submitted.

(c) ACH Information in SRM. The Contractor shall ensure that the ACH information contained in SRM is accurate and complete. The Contractor's failure to maintain accurate and complete information may result in delays in payments.

22. ASSIGNABILITY.

(a) Subject to the terms and conditions of this section the Contract is binding upon the parties and their respective successors and assigns.

(b) The Contractor may not assign, in whole or in part, the Contract or its rights, duties, obligations, or responsibilities hereunder without the prior written consent of the Commonwealth, which consent may not be unreasonably withheld by the Commonwealth, though the Commonwealth may reject the assignment by the Contractor for a legitimate and justifiable reason.

(c) For the purposes of the Contract, the term "assign" shall include, but shall not be limited to, the sale, gift, assignment, encumbrance, pledge, or other transfer of any ownership interest in the Contractor provided, however, that the term shall not apply to the sale or other transfer of stock of a publicly traded company.

(d) Any assignment consented to by the Commonwealth shall be evidenced by a written assignment agreement executed by the Contractor and its assignee in which the assignee agrees to be legally bound by all of the terms and conditions of the Contract and to assume the duties, obligations, and responsibilities being assigned.

(e) Notwithstanding the foregoing, the Contractor may, without the consent of the Commonwealth, assign its rights to payment to be received under the Contract, provided that the Contractor provides written notice of such assignment to the Commonwealth together with a written acknowledgement from the assignee that any such payments are subject to all of the terms and conditions of the Contract.

(f) A change of name by the Contractor, following which the Contractor's federal identification number remains unchanged, is not considered to be an assignment. The Contractor shall give the Commonwealth written notice of any such change of name.

23. INSPECTION AND ACCEPTANCE.

(a) <u>Developed Works and Services</u>.

(i) *Acceptance*. As applicable and upon Commonwealth request, Acceptance of any Developed Work or Service will occur in accordance with an acceptance plan (Acceptance Plan) submitted by the Contactor and approved by the Commonwealth. Upon approval of the Acceptance Plan by the Commonwealth, the Acceptance Plan becomes part of this Contract. A Statement of Work ("SOW") or similar ordering document can contain the Acceptance Plan.

(ii) Reserved.

(iii) If software integration is required at the end of the project, as set out in the Solicitation, the Commonwealth's acceptance of the Software shall be final unless at the time of final acceptance, the Software does not meet the acceptance criteria set forth in the Contract.

(iv) If software integration is not required at the end of the project, as set out in the Solicitation, the Commonwealth's acceptance of the Software shall be complete and final.

(v) *Certification of Completion*. The Contractor shall certify, in writing, to the Commonwealth when an item in the Acceptance Plan is completed and ready for acceptance. Notwithstanding the foregoing, the Commonwealth should consider any Software that has been delivered to be completed and ready for acceptance without further certification from the Contractor. Unless otherwise agreed to by the Commonwealth in the Acceptance Plan, the acceptance period shall be **ten business days** for all items. Following receipt of the Contractor's certification of completion of an item, the Commonwealth shall, either:

(1) Provide the Contractor with Commonwealth's written acceptance of the work product; or

(2) Identify to the Contractor, in writing, the failure of the work product to comply with the specifications, listing all such errors and omissions with reasonable detail.

(vi) *Deemed Acceptance*. If the Commonwealth fails to notify the Contractor in writing of any failures in the work product within the applicable acceptance period, the work product shall be deemed accepted.

(vii) *Correction upon Rejection*. Upon the Contractor's receipt of the Commonwealth's written notice of rejection, which must identify the reasons for the failure of the work product to comply with the specifications, the Contractor shall have **15 business days**, or such other time as the Commonwealth and the Contractor may agree is reasonable, within which to correct all such failures, and resubmit the corrected item, certifying to the Commonwealth, in writing, that the failures have been corrected, and that the items have been brought into compliance with the specifications. Upon receipt of such corrected and resubmitted items and certification, the Commonwealth shall have **30 business days** to test the corrected items to confirm that they are in compliance with the specifications. If the corrected items are in compliance with the specifications, then the Commonwealth shall provide the Contractor with its acceptance of the items in the completed milestone.

(viii) *Options upon Continued Failure*. If, in the opinion of the Commonwealth, the corrected items still contain material failures, the Commonwealth may either:

(1) Repeat the procedure set forth above; or

(2) Proceed with its rights under **Section 28, Termination**, except that the cure period set forth in **Subsection 28(c)** may be exercised in the Commonwealth's sole discretion.

(b) Supplies.

(i) *Inspection prior to Acceptance*. NoSupplies received by the Commonwealth shall be deemed accepted until the Commonwealth has had a reasonable opportunity to inspect the Supplies.

(ii) *Defective Supplies*. Any hardware Supplies discovered to be defective or that fail to conform to the specifications may be rejected upon initial inspection or at any later time if the defects contained in the hardware Supplies or the noncompliance with the specifications were not reasonably ascertainable upon the initial inspection.

(1) The Contractor shall remove rejected Supplies from the premises without expense to the Commonwealth within **15 days** after notification.

(2) Rejected hardware Supplies left longer than **30 days** will be regarded as abandoned, and the Commonwealth shall have the right to dispose of them as its own property and shall retain that portion of the proceeds of any sale which represents the Commonwealth's costs and expenses in regard to the storage and sale of the hardware Supplies.

(3) Upon notice of rejection, the Contractor shall immediately replace all such rejected hardware Supplies with others conforming to the specifications and which are not defective. If the Contractor fails, neglects or refuses to do so, the Commonwealth may procure, in such manner as it determines, supplies similar or identical to the those that Contractor failed, neglected or refused to replace, and deduct from any monies due or that may thereafter become due to the Contractor, the difference between the price stated in the Contract and the cost thereof to the Commonwealth.

24. DEFAULT.

The Commonwealth may, subject to the provisions of **Section 25, Notice of Delays**, and **Section 66, Force Majeure**, and in addition to its other rights under the Contract, declare the Contractor in default by written notice thereof to the Contractor, and terminate (as provided in **Section 28, Termination)** the whole or any part of this Contract for any of the following reasons:

(i) Failure to begin Services within the time specified in the Contract

(ii) Failure to perform the specified Services in accordance with the Contract terms;

(iii) Unsatisfactory performance of the Services not in accordance with the Contract;

(iv) Failure to meet requirements within the time periods(s) specified in the Contract;

(v) Multiple failures over time of a single service level agreement or a pattern of failure over time of multiple service level agreements;

(vi) Failure to provide a Supply or Service that conforms with the specifications referenced in the Contract;

(b)

(i) Failure or refusal to remove material, or remove, replace or correct any Supply rejected as defective or noncompliant;

(ii) Failure to resume a Service, which has been discontinued, within a reasonable time after notice to do so;

(iii) Insolvency;

(iv) Failure or refusal, within **ten days** after written notice by the Contracting Officer, to make payment or show cause why payment should not be made, of any amounts due subcontractors for materials furnished, labor supplied or performed, for equipment rentals or for utility services rendered;

(v) Failure to protect, repair or make good any damage or injury to property of which damage was caused by the Contractor or its agents, employees, or subcontractors;

(vi) Breach of any material provision of this Contract;

(vii) Any breach by Contractor of the security standards or procedures of this Contract;

(viii) Failure to comply with representations made in the Contractor's Proposal; or

25. NOTICE OF DELAYS.

Whenever the Contractor encounters any difficulty that delays or threatens to delay the timely performance of this Contract (including actual or potential labor disputes), the Contractor shall promptly give notice thereof in writing to the Commonwealth stating all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the Commonwealth of any rights or remedies to which it is entitled by law or pursuant to provisions of this Contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay. If an extension of the delivery schedule is granted, it will be done consistent with **Section 27, Changes**.

26. CONDUCT OF SERVICES.

(a) Following the Effective Date of the Contract, Contractor shall proceed diligently with all Services and shall perform such Services with qualified personnel, in accordance with the completion criteria set forth in the Contract.

(b) In determining whether the Contractor has performed with due diligence under the Contract, it is agreed and understood that the Commonwealth may measure the amount and quality of the Contractor's effort against the representations made in the Contractor's Proposal. The Contractor's Services hereunder shall be monitored by the Commonwealth and the Commonwealth's designated representatives. If the Commonwealth actually determines that the Contractor has not performed with due diligence and can substantiate this with demonstratable or written evidence, the Commonwealth and the Contractor will attempt to reach agreement with respect to such matter. Failure of the Commonwealth or the Contractor to arrive at such mutual determinations shall be a dispute concerning a question of fact within the meaning of **Section 30, Contract Controversies**.

27. CHANGES.

(a) At any time during the performance of the Contract, the Commonwealth or the Contractor may request a change to the Contract. Contractor will make reasonable efforts to investigate the impact of the change request on the price, timetable, specifications, and other terms and conditions of the Contract. If the Commonwealth is the requestor of the change, the Contractor will inform the Commonwealth of any charges for investigating the change request prior to incurring such charges. If the Commonwealth and the Contractor agree on the results of the investigation and any necessary changes to the Contract, the parties must complete and execute a change order to modify the Contract and implement the change. The change order will be evidenced by a writing in accordance with the Commonwealth's change order procedures. No work may begin on the change order until the Contractor has received the executed change order. If the parties are not able to agree upon the results of the investigation or the necessary changes to the Contract, a Commonwealth-initiated change request will be implemented at Commonwealth's option and the Contractor shall perform the Services; and either party may elect to have the matter treated as a dispute between the parties under **Section 30, Contract Controversies**. During the pendency of any such dispute, Commonwealth shall pay to Contractor any undisputed amounts.

(b) Changes outside the scope of this Contract shall be accomplished through the Commonwealth's procurement procedures, and may result in an amended Contract or a new contract. No payment will be made for services outside of the scope of the Contract for which no amendment has been executed.

28. TERMINATION.

(a) For Convenience.

(i) The Commonwealth may terminate the Contract, or a Purchase Order issued against the Contract, in whole or in part, without cause by giving Contractor 30 days' prior written notice (Notice of Termination) whenever the

Commonwealth shall determine that such termination is in the best interest of the Commonwealth (Termination for Convenience). Any such termination shall be effected by delivery to the Contractor of a Notice of Termination specifying the extent to which performance under this Contract is terminated either in whole or in part and the date on which such termination becomes effective.

In the event of termination hereunder, Contractor shall receive payment for the following:

(1) all Services performed and Software delivered consistent with the terms of the Contract and applicable governing law prior to the effective date of termination;

(2) all actual and reasonable costs incurred by Contractor as a result of the termination of the Contract; and

In no event shall the Contractor be paid for any loss of anticipated profit (by the Contractor or any subcontractor), loss of use of money, or administrative or overhead costs.

Failure to agree on any termination costs shall be a dispute handled in accordance with **Section 30, Contract Controversies**, of this Contract.

(ii) The Contractor shall cease Services as of the date set forth in the Notice of Termination, and shall be paid only for such Services as have already been satisfactorily rendered up to and including the termination date set forth in said notice, or as may be otherwise provided for in said Notice of Termination, and for such Services performed during the **30-day** notice period, if such Services are requested by the Commonwealth, for the collection, assembling, and transmitting to the Commonwealth of at least all materials, manuals, magnetic media, studies, drawings, computations, maps, supplies, and survey notes including field books, which were obtained, prepared, or developed as part of the Services required under this Contract.

(iii) The above shall not be deemed to limit the Commonwealth's right to terminate this Contract for any reason as permitted by the other provisions of this Contract, or under applicable law.

(b) Non-Appropriation. Any payment obligation or portion thereof of the Commonwealth created by this Contract is conditioned upon the availability and appropriation of funds. When federal, state or local funds are not appropriated or otherwise made available to support continuation of performance or full performance in a subsequent fiscal year period, the Commonwealth shall have the right to terminate the Contract in whole or in part. The Contractor shall be reimbursed in the same manner as that described in subsection (a) to the extent that appropriated funds are available.

(c) Default. The Commonwealth may, in addition to its other rights under this Contract, terminate this Contract in whole or in part by providing written notice of default to the Contractor if the Contractor materially fails to perform its obligations under the Contract and does not cure such failure within **30 days**, or if a cure within such period is not practical, commence a good faith effort to cure such failure to perform within the specified period or such longer period as the Commonwealth may specify in the written notice specifying such failure, and diligently and continuously proceed to complete the cure. The Contracting Officer shall provide any notice of default or written cure notice for Contract terminations.

(i) Reserved.

(ii) Except with respect to defaults of subcontractors, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises out of causes beyond the control of the Contractor. Such causes may include, but are not limited to, acts of God or of the public enemy, fires, floods, epidemics, quarantine restrictions, strikes, work stoppages, freight embargoes, acts of terrorism and unusually severe weather. The Contractor shall notify the Contracting Officer promptly in writing of its inability to perform because of a cause beyond the control of the Contractor.

(iii) Nothing in this subsection (c) shall abridge the Commonwealth's right to suspend, debar or take other administrative action against the Contractor.

(iv) If it is later determined that the Commonwealth erred in terminating the Contract for default, then the Contract shall be deemed to have been terminated for convenience under subsection (a).

(v) If this Contract is terminated as provided by this subsection (c), the Commonwealth may, in addition to any other rights provided in this subsection (c), and subject law and to other applicable provisions of this Contract, require the Contractor to deliver to the Commonwealth in the manner and to the extent directed by the Contracting Officer, such Software, Data, Developed Works, Documentation and other materials as the Contractor has specifically produced or specifically acquired for the performance of such part of the Contract as has been terminated.

(d) The rights and remedies of the Commonwealth provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

(e) The Commonwealth's failure to exercise any rights or remedies provided in this section shall not be construed to be a waiver by the Commonwealth of its rights and remedies in regard to the event of default or any succeeding event of default.

(f) Following exhaustion of the Contractor's administrative remedies as set forth in **Section 30, Contract Controversies**, the Contractor's exclusive remedy shall be to seek damages in the Board of Claims.

29. BACKGROUND CHECKS.

(a) The Contractor, at its expense, must arrange for a background check for each of its employees, as well as the employees of any of its subcontractors, who will have access to Commonwealth Data or Commonwealth facilities (including leased facilities or facilities owned by third parties but utilized by the Commonwealth), either through on-site access or through remote access. Background checks shall be conducted via the Request for Criminal Record Check for in-state Contractor employees or via a criminal background check through the appropriate State Agency for the out of state Contractor employees. The background check shall be conducted prior to initial access by the Contractor employee.

(b) Before the Commonwealth permits access to the Contractor, the Contractor must provide written confirmation that the background checks have been conducted. If, at any time, it is discovered that an employee of the Contractor or an employee of a subcontractor of the Contractor has a criminal record that includes a felony or misdemeanor involving terroristic behavior, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility or which raises concerns about building, system or personal security or is otherwise job-related, the Contractor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee and shall not permit that employee remote access unless the Commonwealth consents to the access, in writing, prior to the access. The Commonwealth may withhold its consent in its sole discretion. Failure of the Contractor to comply with the terms of this section on more than one occasion or Contractor's failure to cure any single failure to the satisfaction of the Commonwealth may result in the Contractor being deemed in default of its Contract.

(c) The Commonwealth specifically reserves the right of the Commonwealth to conduct or require background checks over and above that described herein.

30. CONTRACT CONTROVERSIES.

(a) Pursuant to Section 1712.1 of the *Commonwealth Procurement Code,* 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Contract or a purchase order, the Contractor, within **six months** after the cause of action accrues, must file a written claim with the Contracting Officer for a determination. The claim shall state all grounds upon which the Contractor asserts a controversy exists. If the Contractor fails to file a claim or files an untimely claim, the Contractor is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days** thereafter, either party may request mediation through the Commonwealth Office of General Counsel Dispute Resolution Program, https://www.pa.gov/agencies/ogc/services-provided-to-agencies-home/mediation-home.

(b) If the Contractor or the Contracting Officer requests mediation, and the other party agrees, the Contracting Officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the Contracting Officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the Contracting Officer and the Contractor. The Contracting Officer shall send his/her written determination to the Contractor. If the Contracting Officer fails to issue a final determination within the **120 days** (unless extended by consent of the parties), the claim shall be deemed denied. The Contracting Officer's determination shall be the final order of the purchasing agency.

(c) Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Contractor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Contractor shall proceed diligently with the performance of the Contract or Purchase Order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Contractor pursuant to the terms of the Contract or Purchase Order.

31. CONFIDENTIALITY, PRIVACY AND COMPLIANCE.

(a) General. The Contractor agrees to protect the confidentiality of the Commonwealth's confidential information. The Commonwealth agrees to protect the confidentiality of Contractor's confidential information. Unless the context otherwise clearly indicates the need for confidentiality, information is deemed confidential only when the party claiming confidentiality designates the information as "confidential" in such a way as to give notice to the other party (for example, notice may be communicated by describing the information, and the specifications around its use or disclosure, in the Solicitation or in the Proposal). Neither party may assert that information owned by the other party is such party's confidential information. Notwithstanding the foregoing, all Data provided by, or collected, processed, or created on behalf of the Commonwealth is Confidential Information unless otherwise indicated in writing.

(b) Copying; Disclosure; Termination. The parties agree that confidential information shall not be copied, in whole or in part, or used or disclosed except when essential for authorized activities under this Contract and, in the case of disclosure, where the recipient of the confidential information has agreed to be bound by confidentiality requirements no less restrictive than those set forth herein. Each copy of confidential information shall be marked by the party making the copy with any notices appearing in the original. Upon expiration or termination of this Contract or any license granted hereunder, the receiving party will return to the disclosing party, or certify as to the destruction of, all confidential information in the receiving party's possession, other than one copy (where permitted by law or regulation), which may be maintained for archival purposes only, and which will remain subject to this Contract's security, privacy, data retention/destruction and confidentiality provisions. A material breach of these requirements may result in termination for default pursuant to **Subsection 28(c)**, in addition to other remedies available to the non-breaching party.

(c) Insofar as information is not otherwise protected by law or regulation, the obligations stated in this section do not apply to information:

(i) already known to the recipient at the time of disclosure other than through the contractual relationship;

(ii) independently generated by the recipient and not derived from the information supplied by the disclosing party;

(iii) known or available to the public, except where such knowledge or availability is the result of unauthorized disclosure by the recipient of the proprietary information;

(iv) disclosed to the recipient without a similar restriction by a third party who has the right to make such disclosure; or

(v) required to be disclosed by the recipient by law, regulation, court order, or other legal process.

(d) The Contractor shall use the following process when submitting information to the Commonwealth it believes to be confidential and/or proprietary information or trade secrets:

(i) Prepare and submit an un-redacted version of the appropriate document;

(ii) Prepare and submit a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret. The Contractor shall use a redaction program that ensures the information is permanently and irreversibly redacted; and

(iii) Prepare and submit a signed written statement that identifies confidential or proprietary information or trade secrets and that states:

(1) the attached material contains confidential or proprietary information or trade secrets;

(2) the Contractor is submitting the material in both redacted and un-redacted format, if possible, in accordance with 65 P.S. § 67.707(b); and

(3) the Contractor is requesting that the material be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.

(e) Disclosure of Recipient or Beneficiary Information Prohibited. The Contractor shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from Services under the Contract for any purpose not connected with the Contractor's responsibilities, except with consent pursuant to applicable law or regulations. All material associated with direct disclosures of this kind (including the disclosed information) shall be provided to the Commonwealth prior to the direct disclosure.

(f) Compliance with Laws. Contractor will comply with all applicable laws or regulations related to the use and disclosure of information, including information that constitutes Protected Health Information (PHI) as defined by the *Health Insurance Portability and Accountability* Act (HIPAA). It is understood that **Exhibit A, *Commonwealth of Pennsylvania Business Associate Agreement***, is only applicable if and to the extent indicated in the Contract.

(g) Additional Provisions. Additional privacy and confidentiality requirements may be specified in the Contract.

(h) Restrictions on Use. All Data and all intellectual property provided to the Contractor pursuant to this Contract or collected or generated by the Contractor on behalf of the Commonwealth pursuant to this Contract shall be used only for the work of this Contract. No Data, intellectual property, Documentation or Developed Works may be used, disclosed, or otherwise opened for access by or to the Contractor or any third party unless directly related to and necessary under the Contract.

32. PCI SECURITY COMPLIANCE.

(a) General. By providing the Services under this Contract, the Contractor may create, receive, or have access to credit card records or record systems containing cardholder data including credit card numbers (collectively the "Cardholder Data"). Contractor shall comply with the Payment Card Industry Data Security Standard ("PCI DSS") requirements for Cardholder Data that are prescribed by the payment brands (including, but not limited to, Visa, MasterCard, American Express, and Discover), as they may be amended from time to time. The Contractor acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Contract or as required by applicable law or regulations.

(b) Compliance with Standards. The Contractor shall conform to and comply with the PCI DSS standards as defined by The PCI Security Standards Council at: https://listings.pcisecuritystandards.org/pci_security/. The Contractor shall monitor these PCI DSS standards and will promptly notify the Commonwealth if its practices should not conform to such standards. The Contractor shall provide a letter of certification to attest to meeting this requirement within **seven days** of the Contractor's receipt of the annual PCI DSS compliance report.

33. DATA BREACH OR LOSS.

(a) The Contractor shall comply with all applicable data protection, data security, data privacy and data breach notification laws, including but not limited to the *Breach of Personal Information Notification Act,* 73 P.S. §§ 2301—2330. Further, to the extent the Contractor maintains, stores, or manages computerized data on behalf of the Commonwealth that constitutes personal information, as defined in the *Breach of Personal Information Notification Act,* the Contractor shall comply with the then current version of the following IT Policies (ITPs): Data Classification Policy, IT Security Incident Reporting Policy, and Encryption Policy.

(b) For Data and Confidential Information in the possession, custody, and control of the Contractor or its employees, agents, and/or subcontractors:

(i) The Contractor shall report unauthorized access, use, release, loss, destruction or disclosure of Data or Confidential Information ("Incident") to the Commonwealth within **24 hours** of when the Contractor knows of or reasonably suspects such Incident, and the Contractor must immediately take all reasonable steps to mitigate any potential harm or further access, use, release, loss, destruction or disclosure of such Data or Confidential Information.

(ii) The Contractor shall provide timely notice to all individuals that may require notice under any applicable law or regulation as a result of an Incident. The notice must be pre-approved by the Commonwealth. At the Commonwealth's request, Contractor, at its sole expense, provide credit monitoring services to all individuals that may be impacted by any Incident requiring notice.

(iii) The Contractor shall be solely responsible for any costs, losses, fines, or damages incurred by the Commonwealth due to Incidents.

(c) As to Data and Confidential Information fully or partially in the possession, custody, or control of the Contractor and the Commonwealth, the Contractor shall diligently perform all of the duties required in this section in cooperation with the Commonwealth, until the time at which a determination of responsibility for the Incident, and for subsequent action regarding the Incident, is made final.

34. INSURANCE.

(a) General. Unless otherwise indicated in the Solicitation, the Contractor shall maintain at its expense and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance, issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:

(i) Workers' Compensation Insurance for all of the Contractor's employees and those of any subcontractor engaged in performing Services in accordance with the *Workers' Compensation Act,* Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S.§§ 1—2708.

(ii) Commercial general liability insurance providing coverage from claims for damages for personal injury, death and property of others, including loss of use resulting from any property damage which may arise from its operations under this Contract, whether such operation be by the Contractor, by any agent, contractor or subcontractor, or by anyone directly or indirectly employed by either. The limits of such insurance shall be in an amount not less than **$500,000** per person and **$2,000,000** per occurrence, personal injury and property damage combined. Such policies shall be occurrence based rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or Supplies provided to the Commonwealth.

(iii) Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology activities) in the amount of **$2,000,000**, per accident/occurrence/annual aggregate.

(iv) Professional Liability/Errors and Omissions Insurance in the amount of **$2,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

(v) Network/Cyber Liability Insurance (including coverage for Professional and Technology-Based Services Liability if not covered under Company's

Professional Liability/Errors and Omissions Insurance referenced above) in the amount of **$3,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

(vi) Completed Operations Insurance in the amount of **$2,000,000**, per accident/occurrence/annual aggregate, covering the Contractor, its employees, agents, contractors, and subcontractors in the performance of all services.

(vii) Comprehensive crime insurance in an amount of not less than **$5,000,000** per claim.

(b) Certificate of Insurance. Prior to commencing Services under the Contract, and annually thereafter, the Contractor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days'** prior written notice has been given to the Commonwealth. Such cancellation or change shall not relieve the Contractor of its continuing obligation to maintain insurance coverage in accordance with this section.

(c) Insurance coverage length. The Contractor agrees to maintain such insurance for the latter of the life of the Contract, or the life of any Purchase Orders issued under the Contract.

35. CONTRACTOR RESPONSIBILITY.

(a) Definition. For the purpose of these provisions, the term "Contractor" means as any person, including, but not limited to, a bidder, offeror, loan recipient, grantee or lessor, who has furnished or performed or seeks to furnish or perform, goods, supplies, services, leased space, construction or other activity, under a contract, grant, lease, purchase order or reimbursement agreement with the Commonwealth. The term also includes a permittee, licensee, or any agency, political subdivision, instrumentality, public authority, or other public entity in the Commonwealth.

(b) Contractor Representations.

(i) The Contractor represents for itself and its subcontractors required to be disclosed or approved by the Commonwealth, that as of the date of its execution of this contract, that neither the Contractor, nor any such subcontractors, are under suspension or debarment by the Commonwealth or any governmental entity, instrumentality, or authority and, if the Contractor cannot make this representation, the Contractor shall submit, along with its contract, a written explanation of why such certification cannot be made.

(ii) The Contractor represents that as of the date of its execution of this contract it has no tax liabilities or other Commonwealth obligations, or has filed a timely administrative or judicial appeal if such liabilities or obligations exist, or is subject to a duly approved deferred payment plan if such liabilities exist.

(c) Notification. The Contractor shall notify the Commonwealth if, at any time during the term of this contract, it becomes delinquent in the payment of taxes, or other Commonwealth obligations, or if it or, to the best of its knowledge, any of its subcontractors are suspended or debarred by the Commonwealth, the federal government, or any other state or governmental entity. The Contractor shall provide this notification within 15 days of the date of suspension or debarment.

(d) Default. The Contractor's failure to notify the Commonwealth of its suspension or debarment by the Commonwealth, any other state, or the federal government constitutes an event of default of the contract with the Commonwealth.

(e) Reimbursement. Pursuant to and subject to the limitations of Commonwealth Management Directive 215-09, the Contractor shall reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of State Inspector General for investigations of the Contractor's compliance with the terms of this contract or any other agreement between the Contractor and the Commonwealth that results in the suspension or debarment of the Contractor. These costs include, but are not limited to, salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

(f) Suspension and Debarment List. The Contractor may obtain a current list of suspended and debarred Commonwealth contractors by visiting the eMarketplace website at http://www.emarketplace.state.pa.us and clicking the Debarment list tab.

36. OFFSET PROVISION FOR COMMONWEALTH CONTRACTS.

Pursuant to and subject to the limitations of Commonwealth Management Directive 215-09, the Commonwealth may set off the amount of any state tax liability or other obligation of the Contractor, or its subsidiaries, owed to the Commonwealth against any payments due the Contractor under any contract between the Commonwealth and Contractor.

37. TAXES-FEDERAL, STATE AND LOCAL.

The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-7400001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.

38. LIMITATION OF LIABILITY.

(a) General. The Contractor's liability to the Commonwealth under this shall be limited to the greater of **$250,000** or the value of all orders issued under this Contract in the immediately preceding twelve months. This limitation will apply, except as otherwise stated in this Contract, regardless of the form of action, whether in contract or in tort, including negligence. This limitation does not, however, apply to any damages:

(i) for bodily injury;

(ii) for death;

(b) for gross negligence or intentional or willful misconduct;

(i) for damage to real property or tangible personal property for which the Contractor is legally liable;

(ii) to Contractor's indemnity obligations under this Contract.

(iii) under **Section 42, Patent, Copyright, Trademark and Trade Secret Protection**;

(iv) under **Section 33, Data Breach or Loss,** for which the limitation shall be the greater of **$7,500,000** or 10 times the value of all orders issued under this Contract in the immediately preceding twelve months; or

(c) under **Section 41, Virus, Malicious, Mischievous or Destructive Programming,** for which the limitation shall be the greater of **$7,500,000** or 10 times the value of all orders issued under this Contract in the immediately preceding twelve months.

(d) The Contractor will not be liable for consequential or incidental damages, except for damages as set forth in **paragraphs (a)(i)—(viii)** above, or as otherwise specified in the Contract.

39. INDEMNIFICATION.

(a) Contractor Obligations. The Contractor shall indemnify the Commonwealth against all third-party claims, suits, demands, losses, damages, costs, and expenses, including reasonable litigation expenses, attorneys' fees, and liabilities, arising out of or in connection with any activities performed by the Contractor or its employees and agents that are related to this contract.

(b) Commonwealth Attorneys Act. The Commonwealth shall provide the Contractor with prompt notice of any claim or suit of which it learns. Pursuant to the Commonwealth Attorneys Act (71 P.S. Section 732-101, et seq.), the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under any terms as it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits.

(c) Settlement. Notwithstanding the above, neither party may enter into a settlement of any claim or suit without the other party's written consent, which will not be unreasonably withheld. The Commonwealth may, in its sole discretion, allow the Contractor to control the defense and any related settlement negotiations.

40. SOVEREIGN IMMUNITY.

No provision of this Contract may be construed to waive or limit the sovereign immunity of the Commonwealth of Pennsylvania or its governmental sub-units.

41. VIRUS, MALICIOUS, MISCHIEVOUS OR DESTRUCTIVE PROGRAMMING.

(a) The Contractor shall be liable for any damages incurred by the Commonwealth if the Contractor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commonwealth’s software or computer networks and has failed to comply with the applicable Commonwealth software security standards. The Commonwealth must demonstrate that the Contractor or any of its employees, subcontractors or consultants introduced the virus or malicious, mischievous or destructive programming. The Contractor’s liability shall cease if the Commonwealth has not fully complied with its own software security standards.

(b) The Contractor shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the Contractor’s failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Contractor or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of Software by the Contractor or any of its employees, agents, subcontractors, or consultants, the Contractor shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

(d) The Contractor shall be responsible for reviewing Commonwealth software security standards and complying with those standards when applicable to the Contractor's performance under a Purchase Order or Statement of Work.

(e) The Commonwealth may, upon at least thirty (30) days' prior notice to Contractor, audit any computing devices being used by representatives of the Contractor to provide Services to the Commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commonwealth network until the proper installations have been made

(f) The Contractor may use the anti-virus software used by the Commonwealth to protect Contractor's computing devices used in the course of providing services to the Commonwealth. It is understood that the Contractor may not install the software on any computing device not being used to provide services to the Commonwealth, and that all copies of the software will be removed from all devices upon termination of this Contract.

(g) The Commonwealth will not be responsible for any damages to the Contractor's computers, data, software, etc. caused as a result of the installation of the Commonwealth's anti-virus software or monitoring software on the Contractor's computers unless the Commonwealth requires the Contractor to use the specified anti-virus software.

42. PATENT, COPYRIGHT, TRADEMARK AND TRADE SECRET PROTECTION.

(a) The Contractor shall hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States or foreign patents, copyrights, trademarks or trade dress, or for a misappropriation of trade secrets arising out of performance of this Contract, including all work, services, materials, reports, studies, and computer programs provided by the Contractor, and in any such suit or proceeding will satisfy any final award for such infringement, including costs. The Commonwealth agrees to give Contractor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act*, Act of

October 15, 1980, P.L. 950, No. 164, as amended, 71 P.S. § 732-101—732-506, the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion and under the terms it deems appropriate, may delegate its right of defense. If OAG delegates the defense to the Contractor, the Commonwealth will cooperate with all reasonable requests of Contractor made in the defense of such suits. No settlement that prevents the Commonwealth from continuing to use the Developed Works as provided herein shall be made without the Commonwealth's prior written consent. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Contractor that, in the event it requests that the Commonwealth provide support to the Contractor in defending any such claim, the Contractor shall reimburse the Commonwealth for all expenses (including attorneys' fees, if such are made necessary by the Contractor's request) incurred by the Commonwealth for such support. If OAG does not delegate the defense of the matter, the Contractor's obligation to indemnify ceases. The Contractor, at its expense, will provide whatever cooperation OAG requests in the defense of the suit.

(b) The Contractor agrees to exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Contractor agrees that, in all respects applicable to this Contract, it has exercised and will continue to exercise due diligence to ensure that all works produced under this Contract do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties. The Contractor also agrees that work produced for the Commonwealth under this contract shall be free and clear from all claims of any nature.

(c) If the defense of the suit is delegated to the Contractor, the Contractor shall pay all damages and costs awarded therein against the Commonwealth. If information and assistance are furnished by the Commonwealth at the Contractor's written request, it shall be at the Contractor's expense, but the responsibility for such expense shall be only that within the Contractor's written authorization.

(d) If, in the Contractor's opinion, the products, materials, reports, studies, or computer programs furnished hereunder are likely to or do become subject to a claim of infringement of a United States patent, copyright, trademark or trade dress, or for a misappropriation of trade secret, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, at its option and expense:

(i) substitute functional equivalents for the alleged infringing products, materials, reports, studies, or computer programs; or

(ii) obtain the rights for the Commonwealth to continue the use of such products, materials, reports, studies, or computer programs.

(e) If any of the products, materials, reports, studies, or computer programs provided by the Contractor are in such suit or proceeding held to constitute infringement and the use or publication thereof is enjoined, the Contractor shall, at its own expense and at its option, either procure the right to publish or continue use of such infringing products, materials, reports, studies, or computer programs, replace them with non-infringing items, or modify them so that they are no longer infringing.

(f) If the Contractor is unable to do any of the preceding, the Contractor agrees to pay the Commonwealth:

(i) any amounts paid by the Commonwealth less a reasonable amount based on the acceptance and use of the deliverable;

(ii) any license fee less an amount for the period of usage of any software; and

(iii) the prorated portion of any service fees representing the time remaining in any period of service for which payment was made.

(g) Notwithstanding the above, the Contractor shall have no obligation for:

(i) modification of any product, service, or deliverable provided by the Commonwealth;

(ii) any material provided by the Commonwealth to the Contractor and incorporated into, or used to prepare, a product, service, or deliverable;

(iii) use of the product, service, or deliverable in other than its specified operating environment;

(iv) the combination, operation, or use of the product, service, or deliverable with other products, services, or deliverables not provided by the Contractor as a system or the combination, operation, or use of the product, service, or deliverable, with any products, data, or apparatus that the Contractor did not provide;

(v) infringement of a non-Contractor product alone;

(vi) the Commonwealth's distribution, marketing or use beyond the scope contemplated by the Contract; or

(vii) the Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Contractor at no charge.

(h) The obligation to indemnify the Commonwealth, under the terms of this section, shall be the Contractor's sole and exclusive obligation for the infringement or misappropriation of intellectual property.

43. CONTRACT CONSTRUCTION.

The provisions of this Contract shall be construed in accordance with the provisions of all applicable laws and regulations of the Commonwealth. However, by executing this Contract, the Contractor agrees that it has and will continue to abide by the intellectual property laws and regulations of the United States of America.

44. USE OF CONTRACTOR AND THIRD PARTY PROPERTY.

(a) Definitions.

(i) "Contractor Property" refers to Contractor-owned tangible and intangible property.

(ii) "Third Party" refers to a party that licenses its property to Contractor for use under this Contract.

(iii) "Third Party Property" refers to property licensed by the Contractor for use in its work under this Contract.

(b) Contractor Property shall remain the sole and exclusive property of the Contractor. Third Party Property shall remain the sole and exclusive property of the Third Party. The Commonwealth acquires rights to the Contractor Property and Third Party Property as set forth in this Contract.

(i) Intentionally Omitted.

(ii) If Third Party Property is integrated into the Supplies or Services which are not Developed Works, or the Third Party Property is otherwise necessary for the Commonwealth to attain the full benefit of the Supplies or Services in accordance with the terms of the Contract, the Contractor shall gain the written approval of the Commonwealth prior to the use of the Third Party Property or the integration of the Third Party Property into the Supplies or Services. Third Party Property approved by the Commonwealth is hereby licensed to the Commonwealth as necessary to meet the Contract requirements.

(iii) If the Third Party requires a separate license agreement, the license terms shall be acceptable to the Commonwealth and will be separately negotiated and executed between the Commonwealth and the Third Party.

(iv) If the use or integration of the Third Party Property is not approved in writing under this section, the Third Party Property shall be deemed to be licensed under paragraph (b)(i) above.

(v) If the Contract expires or is terminated for default pursuant to **Subsection 28(c)** before the Contract requirements are complete, all rights are granted for a duration and for purposes necessary to facilitate Commonwealth's or a Commonwealth-approved vendor's completion of the Supplies, Services or Developed Works under this Contract. The Contractor, in the form used by Contractor in connection with the Supplies, Services, or Developed Works, shall deliver to Commonwealth the object code version of such Contractor Property, the Third Party Property and associated licenses immediately prior to such expiration or termination to allow the Commonwealth to complete such work.

(vi) Where third party users are reasonably anticipated by the Contract, all users are granted the right to access and use Contractor Property for the purposes of and within the scope indicated in the Contract.

(c) The Commonwealth will limit its agents and contractors' use and disclosure of the Contractor Property as necessary to perform work on behalf of the Commonwealth.

(d) The parties agree that the Commonwealth, by acknowledging the Contractor Property, does not agree to any terms and conditions of the Contractor Property agreements that are inconsistent with or supplemental to this Contract unless separately negotiated and executed as part of a properly executed amendment to the Contract.

(e) Reports. When a report is provided under this Contract, but was not developed specifically for the Commonwealth under this Contract, the ownership of the report will remain with the Contractor; provided, however, that the Commonwealth has the right to use, copy and distribute the report within the executive agencies of the Commonwealth.

45. USE OF COMMONWEALTH PROPERTY.

"Commonwealth Property" refers to Commonwealth-owned Software, Data and property (including intellectual property) and third party owned Software and property (including intellectual property) licensed to the Commonwealth.

(a) Confidentiality of Commonwealth Property. All Commonwealth Property provided to the Contractor pursuant to this Contract or collected or generated by the Contractor on behalf of the Commonwealth pursuant to this Contract shall be considered confidential information under **Section 31, Confidentiality, Privacy, and Compliance**.

(b) License grant and restrictions. During the term of this Contract, Commonwealth grants to Contractor and its subcontractors for the limited purpose of providing the Services covered under this Contract, a limited, nonexclusive, nontransferable, royalty-free right (subject to the terms of any third party agreement to which the

Commonwealth is a party) to access, use, reproduce, and modify Commonwealth Property in accordance with the terms of the Contract. The Commonwealth's license to Contractor is limited by the terms of this Contract.

(i) The Contractor hereby assigns to the Commonwealth its rights, if any, in any derivative works resulting from Contractor's modification of the Commonwealth Intellectual Property. Contractor agrees to execute any documents required to evidence this assignment and to waive any moral rights and rights of attribution provided for in Section 106A of Title 17 of the United States Code, the *Copyright Act of 1976,* as amended.

(ii) Neither Contractor nor any of its subcontractors may decompile or reverse engineer, or attempt to decompile or reverse engineer, any of the Commonwealth Intellectual Property. Commonwealth hereby represents that it has the authority to provide the license grant and rights set forth in this section.

(c) Reservation of rights. All rights not expressly granted here to Contractor are reserved by the Commonwealth.

(d) Termination of Commonwealth license grant.

(i) *Rights Cease*. Upon the expiration or termination for any reason of Contractor's obligation to provide the Services under this Contract, all rights granted to Contractor under this section shall immediately cease.

(ii) *Return Commonwealth Property*. Contractor shall, at no cost to Commonwealth, deliver to Commonwealth all of the Commonwealth Intellectual Property (including any related source code then in Contractor's possession or under its control) in the form in use as of the Effective Date of such expiration or termination (except that Commonwealth Data shall be turned over in a form acceptable to the Commonwealth).

(iii) *List of utilized Commonwealth Property/Destruction*. Within **15 days** after termination, Contractor shall provide the Commonwealth with a current copy of the list of Commonwealth Intellectual Property in use as of the date of such expiration or termination. Concurrently therewith, Contractor shall destroy or erase all other copies of any of the Commonwealth Software then in Contractor's possession or under its control unless otherwise instructed by Commonwealth, in writing; provided, however, that Contractor may retain one archival copy of such Commonwealth Software, until final resolution of any actively asserted pending disputes between the Parties, such retention being for the sole purpose of resolving such disputes.

(e) Effect of license grant termination. Consistent with the provisions of this section, Contractor shall refrain from manufacturing, copying, marketing, distributing or using any Commonwealth Software or any other work which incorporates the Commonwealth Software.

(f) Commonwealth Property Protection.

(i) Contractor acknowledges Commonwealth's exclusive right, title and interest, including without limitation copyright and trademark rights, in and to Commonwealth Data, Commonwealth Software and the Developed Works developed under the provisions of this Contract, and Contractor shall not, directly or indirectly, do or cause to be done any act or thing contesting or in any way impairing or tending to impair any part of said right, title, and interest, and shall not use or disclose the Commonwealth Data, Commonwealth Software or the Developed Works without Commonwealth's written consent, which consent may be withheld by the Commonwealth for any reason.

(ii) Contractor shall not, in any manner, represent that Contractor has any ownership interest in the Commonwealth Data, Commonwealth Software or the Developed Works other than as agreed upon in the applicable Purchase Order or SOW. However, Metadata may specifically be used to improve the Service being offered to the Commonwealth under an applicable Order.

46. OWNERSHIP OF DEVELOPED WORKS.

Unless otherwise specified in the Contract, including the Solicitation, ownership of all Developed Works shall be in accordance with the provisions set forth in this section.

(a) Rules for usage for Developed Works.

(i) *Property of Contractor.* If Developed Works modify, improve, contain, or enhance application software programs or other materials generally licensed by the Contractor, then such Developed Works shall be the property of the Contractor, and Contractor hereby grants Commonwealth an irrevocable, nonexclusive, worldwide, fully paid-up license (to include source code and relevant documentation) in perpetuity to use, modify, execute, reproduce, display, perform, prepare derivative works from and distribute, within the Commonwealth, such Developed Works.

(1) For purposes of distribution under the license grant created by this section, Commonwealth includes any government agency, department, instrumentality, division, unit or other office that is part of the Commonwealth of Pennsylvania, together with the State System of Higher Education (including any of its universities), any county, borough, commonwealth, city, municipality, town, township special purpose district, or other similar type of

governmental instrumentality located within the geographical boundaries of the Commonwealth of Pennsylvania.

(2) If federal funds are used in creation of the Developed Works, the Commonwealth also includes any other state government as well as the federal government.

(ii) *Property of Commonwealth/licensor*. If the Developed Works modify, improve or enhance application software or other materials not licensed to the Commonwealth by the Contractor, then such modifications, improvements and enhancements shall be the property of the Commonwealth or its licensor.

(b) <u>Copyright Ownership</u>.

(i) *Works made for hire; general*. Except as indicated in paragraph (a)(i), above, Developed Works developed as part of the scope of work for the Project, including Developed Works developed by subcontractors, are the sole and exclusive property of the Commonwealth and shall be considered “works made for hire” under the *Copyright Act of 1976*, as amended, 17 United States Code.

(ii) *Assignment*. In the event that the Developed Works do not fall within the specifically enumerated works that constitute works made for hire under the United States copyright laws, Contractor agrees to assign and, upon their authorship or creation, expressly and automatically assigns, all copyright interests, proprietary rights, trade secrets, and other right, title, and interest in and to such Developed Works to Commonwealth. Contractor further agrees that it will have its subcontractors assign, and upon their authorship or creation, expressly and automatically assigns all copyright interest, proprietary rights, trade secrets, and other right, title, and interest in and to the Developed Works to the Commonwealth.

(iii) *Rights to Commonwealth*. When the Commonwealth solicits for Developed Works under this Contract, Commonwealth shall have all rights accorded an owner of copyright under the United States copyright laws including, but not limited to, the exclusive right to reproduce the Developed Works in multiple copies, the right to distribute copies by sales or other transfers, the right to register all copyrights in its own name as author in the United States and in foreign countries, the right to prepare derivative works based upon the Developed Works and the right to display the Developed Works. .

(iv) *Intentionally Omitted.*

(v) *Completion or termination of Contract*. Upon completion or termination of this Contract, Developed Works, or completed portions thereof, shall immediately be delivered by Contractor to the Commonwealth.

(vi) *Warranty of noninfringement*. Contractor represents and warrants that, to the best of its knowledge, information, and belief the Developed Works are original and do not infringe any copyright, patent, trademark, or other intellectual property right of any third party and are in conformance with the intellectual property laws and regulations of the United States.

(c) Patent ownership. Except as set forth in the applicable SOW or ither ordering document, Contractor and its subcontractors shall retain ownership to patentable items, patents, processes, inventions or discoveries (collectively, the Patentable Items) made by the Contractor during the performance of this Contract. Notwithstanding the foregoing, the Commonwealth shall be granted a nonexclusive, nontransferable, royalty free license to use or practice the Patentable Items. Commonwealth may disclose to third parties any such Patentable Items made by Contractor or any of its subcontractors under the scope of work for the Project that have been previously publicly disclosed. Commonwealth understands and agrees that any third party disclosure will not confer any license to such Patentable Items.

(d) Federal government interests. Certain funding under this Contract may be provided by the federal government. Accordingly, the rights to Developed Works or Patentable Items of Contractors or subcontractors hereunder will be further subject to government rights as set forth in 37 C.F.R. Part 401, as amended, and other applicable law or regulations.

(e) Usage rights. Except as otherwise covered by this section either Party, in the ordinary course of conducting business, may use any ideas, concepts, know-how, methodologies, processes, components, technologies, algorithms, designs, modules or techniques relating to the Services.

(f) Contractor's copyright notice obligations. Contractor will affix the following Copyright Notice to the Developed Works developed under this section and all accompanying documentation: "*Copyright © [year] by the Commonwealth of Pennsylvania. All Rights Reserved*." This notice shall appear on all versions of the Developed Works delivered under this Contract and any associated documentation. It shall also be programmed into any and all Developed Works delivered hereunder so that it appears at the beginning of all visual displays of such Developed Works.

47. SOURCE CODE AND ESCROW ITEMS OBLIGATIONS.

RESERVED

48. CONTRACTOR HOSTED SECURITY, LOCATION, STATUS AND DISPOSITION OF DATA.

Unless the Solicitation specifies otherwise:

(i) All Data must be stored within the United States;

(ii) The Contractor shall be responsible for maintaining the privacy, security and integrity of Data in the Contractor's or its subcontractors' possession;

(iii) All Data shall be provided to the Commonwealth upon request, in a form acceptable to the Commonwealth and at no cost or shall be readily available to the Commonwealth for on-demand exporting during the applicable period of performance;

(iv) Any Data shall be destroyed by the Contractor at the Commonwealth's request;

(v) Any Data shall be held for litigation or public records purposes by the Contractor at the Commonwealth's request, and in accordance with the security, privacy and accessibility requirements of this Contract; and

(vi) The Contractor shall comply with the applicable provisions set forth in **Exhibit B, Requirements for Non-Commonwealth Hosted Applications/Services**.

49. PUBLICATION RIGHTS AND/OR COPYRIGHTS.

(a) Except as otherwise provided in **Section 46, Ownership of Developed Works**, the Contractor shall not publish any of the results of the work without the written permission of the Commonwealth. The publication shall include the following statement: "The opinions, findings, and conclusions expressed in this publication are those of the author and not necessarily those of the Commonwealth of Pennsylvania." The Contractor shall not include in the documentation any copyrighted matter, unless the Contractor provides the Commonwealth with written permission of the copyright owner.

(b) Except as otherwise provided in the Contract, the Commonwealth shall have authority to reproduce, distribute, and use any submitted non-proprietary report or data designed or developed and delivered to the Commonwealth as part of the performance of the Contract.

50. CHANGE IN CONTRACTOR'S OWNERSHIP.

In the event that the Contractor should change ownership, the Commonwealth shall have the exclusive option of:

(i) continuing under the terms and conditions of this Contract with the Contractor or its successors or assigns for the full remaining term of this Contract;

(ii) continuing under the terms and conditions of this Contract with the Contractor or its successors or assigns for such period of time as is necessary to replace the products, materials, reports, studies, or computer programs; or

(b) immediately terminating this Contract.

51. OFFICIALS NOT TO BENEFIT.

No official or employee of the Commonwealth and no member of its General Assembly who exercises any functions or responsibilities under this Contract shall participate in any decision relating to this Contract which affects their personal interest or the interest of any corporation, partnership, or association in which they are, directly or indirectly, interested; nor shall any such official or employee of the Commonwealth or member of its General Assembly have any interest, direct or indirect, in this Contract or the proceeds thereof.

52. COMPLIANCE WITH LAWS.

(a) The Contractor shall comply with all federal, state and local laws, regulations and policies applicable to its Services or Supplies, including, but not limited to, all statutes, regulations and rules that are in effect as of the Effective Date of the Contract and shall procure at its expense all licenses and all permits necessary for the fulfillment of its obligation applicable to its Services, Supplies, or performance under the Contract.

(b) If any existing law, regulation or policy is changed or if any new law, regulation or policy is enacted that affects the Services or Supplies provided under this Contract, the Parties shall modify this Contract, via **Section 27, Changes**, to the extent reasonably necessary to:

(i) Ensure that such Services or Supplies will be in full compliance with such laws, regulations and policies; and

(ii) Modify the rates applicable to such Services or Supplies, unless otherwise indicated in the Solicitation.

53. AMERICANS WITH DISABILITIES ACT.

(a) <u>No Exclusion</u>. Pursuant to the Americans with Disabilities Act, 42 U.S. Code § 12101, et seq., no qualified individual with a disability may, on the basis of the disability, be excluded from participation in this contract or from activities provided for under this contract.

(b) Compliance. For all goods and services provided pursuant to this contract, the Contractor shall comply with Title II of the Americans with Disabilities Act, the "General Prohibitions Against Discrimination" set forth in 28 C. F. R. § 35.130, and all other regulations promulgated under Title II of the Americans with Disabilities Act that apply to state and local governments.

(c) Indemnification. Pursuant to and subject to the limitations of Commonwealth Management Directive 215.12, the Contractor shall indemnify the Commonwealth against all third-party claims, suits, demands, losses, damages, costs, and expenses, including without limitation, litigation expenses, attorneys' fees, and liabilities, arising out of or in connection with the Contractor's failure or its employee's or agent's failure to comply with the provisions of paragraph a, as determined by the Commonwealth in its sole discretion.

54. EXAMINATION OF RECORDS.

(a) The Contractor agrees to maintain, using its standard procedures, and in accordance with Generally Accepted Accounting Principles, books, records, documents, and other evidence pertaining to the charges under this Contract to the extent and in such detail as will properly reflect all charges for which reimbursement is claimed under the provisions of this Contract.

(b) The Contractor agrees to make available at the office of the Contractor with at least one business week's notice and no more than once per year, during regular business hours during the term of this Contract and the period set forth in subsection (c) below, any of the records for inspection, audit, or reproduction by any authorized Commonwealth representative. To the extent allowed by applicable laws or regulations, the Commonwealth agrees to maintain any documents so provided in accordance with the confidentiality provisions in **Section 31, Confidentiality, Privacy and Compliance**.

(c) The Contractor shall preserve and make available its records for a period of **three years** from the date of final payment under this Contract.

(i) If this Contract is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for a period of **three years** from the date of any resulting final settlement.

(ii) Non-privileged records which relate to litigation or the settlement of claims arising out of the performance of this Contract, or charges under this Contract as to which exception has been taken by the auditors, shall be retained by the Contractor until such litigation, claims, or exceptions have been finally resolved.

(d) Except for documentary evidence retained pursuant to paragraph (c)(ii) above, the Contractor may in fulfillment of its obligation to retain its records as required by this section substitute photographs, microphotographs, or other authentic reproductions of such records, after the expiration of **two years** following the last day of the month of reimbursement to the Contractor of the invoice or voucher to which such records relate, unless a shorter period is authorized by the Commonwealth with the concurrence of its auditors.

(e) The provisions of this section shall be applicable to and sufficiently agreed to by the Contractor with their Subcontractors.

55. SINGLE AUDIT ACT OF 1984.

In compliance with the *Single Audit Act of 1984*, as amended, the Contractor agrees to the following:

(a) This Contract is subject to audit by federal and state agencies or their authorized representative in accordance with the auditing standards promulgated by the Comptroller General of the United States and specified in the most current version of *Government Auditing Standards* (Yellow Book).

(b) The audit requirement of this Contract will be satisfied if a single audit is performed under the provisions of the *Single Audit Act of 1984*, as amended, 31 U.S.C. § 7501, *et seq*., and all rules and regulations promulgated pursuant to the Act.

(c) The Commonwealth reserves the right for federal and state agencies or their authorized representatives to perform additional audits of a financial/compliance, economy/efficiency, or program results nature, if deemed necessary.

(d) The Contractor further agrees to comply with applicable requirements if they are issued by the state agency upon receipt of additional guidance received from the federal government regarding the *Single Audit Act of 1984*, as amended.

56. AGENCY-SPECIFIC SENSITIVE AND CONFIDENTIAL COMMONWEALTH DATA (IF APPLICABLE).

(a) Contractor understands that its level of access may allow or require it to view or access highly sensitive and confidential Commonwealth and third party data. This data is subject to various state and federal laws, regulations and policies that vary from agency to agency, and from program to program within an agency. If applicable, prior to deployment of the Supplies or Services, the Contractor must receive and sign off on particular instructions and limitations as dictated by that Commonwealth agency, including but not limited to, as necessary, HIPAA Business Associate Agreements. This sign-off document, a sample of which is attached as **Exhibit C, Sample Sign-off Document**, will include a description of the nature of the data which may be implicated based on the nature of the Contractor's access, and will incorporate the Business Associate Agreement if it is applicable.

(b) The Contractor hereby certifies and warrants that, after being informed by the Commonwealth agency of the nature of the data which may be implicated and prior to the deployment of the Supplies or Services, the Contractor is and shall remain compliant with all applicable state and federal laws, regulations and policies regarding the data's protection, and with the requirements memorialized in every completed and signed sign-off document. Every sign-off document completed by a Commonwealth agency and signed by at least one signatory authorized to bind the Contractor is valid and is hereby integrated and incorporated by reference into this Contract.

(c) This section does not require a Commonwealth agency to exhaustively list the laws, regulations or policies to which implicated data is subject; the Commonwealth agency is obligated only to list the nature of the data implicated by the Contractor's access, to refer the Contractor to its privacy and security policies, and to specify requirements, regulations, or policies that are not otherwise inherent in compliance with applicable laws and regulations which are well-recognized and understood as industry standard and applicable to the Commonwealth's data classification.

(d) The requirements of this section are in addition to and not in lieu of other requirements of this Contract, its Exhibits, Appendices and Attachments, having to do with data privacy and security, including but not limited to the requirement that the Contractor comply with all applicable Commonwealth ITPs, which can be found at https://www.pa.gov/agencies/oa/policies/it-policies.

(e) Contractor shall conduct additional background checks, in addition to those required in **Section 29, Background Checks**, when applicable and specifically requested by a Commonwealth agency in its sign-off documents.

57. FEDERAL REQUIREMENTS.

If applicable, the Contractor must receive and sign off on particular federal requirements that a Commonwealth agency may be required to include when utilizing federal funds to procure the Supplies and Services. This sign-off document, in addition to any applicable requirements of **Section 56, Agency-Specific Sensitive and Confidential Commonwealth Data**, will include a description of the required federal provisions, along with the applicable forms necessary for the Contractor and/or Software Licensor to execute, as necessary. Every sign-off document completed by a Commonwealth agency and signed by at least one signatory authorized to bind the Contractor is valid and is hereby integrated and incorporated by reference into this Contract. A sample sign-off document is attached to these Terms as **Exhibit C, Sample Sign-off Document**.

58. ADDITIONAL FEDERAL PROVISIONS.

Additional contract provisions may be incorporated into this Contract pursuant to federal law, regulation or policy.

59. ENVIRONMENTAL PROTECTION.

In carrying out this Contract, the Contractor shall minimize pollution and shall strictly comply with all applicable environmental laws and regulations, including the *Clean Streams Law,* Act of June 22, 1937 (P.L. 1987, No. 394), as amended, 35 P.S. §§ 691.1—691.801; the *Solid Waste Management Act,* Act of July 7, 1980 (P.L. 380, No. 97), as amended, 35 P.S. §§ 6018.101—68.1003; and the *Dam Safety and Encroachment Act,* Act of November 26, 1978 (P.L. 1375, No. 325), as amended, 32 P.S. §§ 693.1—693.27.

60. NONDISCRIMINATION/SEXUAL HARASSMENT.

(a) Representations. The Contractor represents that it is presently in compliance with and will remain in compliance with all applicable federal, state, and local laws, regulations, and policies relating to nondiscrimination and sexual harassment for the term of the contract. The Contractor shall, upon request and within the time periods requested by the Commonwealth, furnish all necessary employment documents and records, including EEO-1 reports, and permit access to its books, records, and accounts by the Commonwealth for the purpose of ascertaining compliance with provisions of this Nondiscrimination/Sexual Harassment Clause.

(b) Nondiscrimination/Sexual Harassment Obligations. The Contractor shall not:

(i) in any manner discriminate in the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under this contract or any subcontract, by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the Pennsylvania Human Relations Act ("PHRA") and applicable federal laws, against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.

(ii) in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the PHRA and applicable federal laws, against or intimidate any employee involved in the manufacture of supplies, the performance of work, or any other activity required under this contract.

(iii) in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the PHRA and applicable federal laws, in the provision of services under this contract.

(iv) in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of PHRA and applicable federal laws, against any subcontractor or supplier who is qualified to perform the work to which this contract relates.

(v) in any manner discriminate against employees by reason of participation in or decision to refrain from participating in labor activities protected under the Public Employee Relations Act, Pennsylvania Labor Relations Act or National Labor Relations Act, as applicable and to the extent determined by entities charged with such Acts' enforcement and shall comply with any provision of law establishing organizations as employees' exclusive representatives.

(c) Establishment of Contractor Policy. The Contractor shall establish and maintain a written nondiscrimination and sexual harassment policy that complies with the applicable law and these Nondiscrimination/Sexual Harassment provisions and shall inform its employees in writing of the policy. The policy must contain a provision that states that sexual harassment will not be tolerated and employees who practice it will be disciplined. For the entire period of the contract, the Contractor shall: (1) post its written nondiscrimination and sexual harassment policy or these Nondiscrimination/Sexual Harassment provisions conspicuously in easily accessible and well-lighted places customarily frequented by employees at or near where the contracted services are performed; or (2) provide electronic notice of the policy or this clause to its employees not less than annually.

(d) Notification of Violations. The Contractor's obligations pursuant to these provisions are ongoing from the effective date and through the termination date of the contract. Accordingly, the Contractor shall notify the Commonwealth if, at any time during the term of this contract, it becomes aware of any actions or occurrences that would result in violation of these provisions.

(e) Cancellation or Termination of Contract. The Commonwealth may cancel or terminate this contract and all money due or to become due under this contract may be forfeited for a violation of the terms and conditions of these Nondiscrimination/Sexual Harassment provisions. In addition, the agency may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File.

(f) Subcontracts. The Contractor shall include the requirements of these Nondiscrimination/Sexual Harassment provisions in its contracts with all subcontractors providing goods or services under this contract. The incorporation of these requirements in the Contractor's subcontracts does not create privity of contract between the Commonwealth and any subcontractor, and no third-party beneficiaries are created by those provisions. If the Contractor becomes aware of a subcontractor's violation of these requirements, the Contractor shall use its best efforts to ensure the subcontractor's compliance with these requirements.

61. CONTRACTOR INTEGRITY.

(a) Definitions. For purposes of these Contractor Integrity Provisions, the following definitions apply:

(i) "Affiliate" means two or more entities where (a) a parent entity owns more than 50% of the voting stock of each of the entities; (b) a common shareholder or group of shareholders owns more than 50% of the voting stock of each of the entities; or (c) the entities have a common proprietor or general partner.

(ii) "Contractor" means the individual or entity, that has entered into this contract with the Commonwealth.

(iii) "Contractor Related Parties" means any Affiliates of the Contractor and the Contractor's executive officers, Pennsylvania officers and directors, or owners of five percent or more interest in the Contractor.

(iv) "Financial Interest" means ownership of more than a five percent interest in any business or holding a position as an officer, director, trustee, partner, employee, or holding any position of management.

(v) "Gratuity" means tendering, giving, or providing anything of more than nominal monetary value including, but not limited to, cash, travel, entertainment, gifts, meals, lodging, loans, subscriptions, advances, deposits of money, services, employment, or contracts of any kind. The exceptions set forth in the Governor's Code of Conduct, Executive Order 1980-18, as may be amended, 4 Pa. Code §7.153(b), apply.

(vi) "Non-bid Basis" means a contract awarded or executed by the Commonwealth with Contractor without seeking bids or proposals from any other potential bidder or offeror.

(b) Representations and Warranties.

(i) Contractor Representation and Warranties. The Contractor represents, to the best of its knowledge and belief, and warrants that within the last five years neither the Contractor nor Contractor Related Parties have:

(1) been indicted or convicted of a crime involving moral turpitude or business honesty or integrity in any jurisdiction;
(2) been suspended, debarred, or otherwise disqualified from entering into any contract with any governmental agency;
(3) had any business license or professional license suspended or revoked;
(4) had any sanction or finding of fact imposed as a result of a judicial or administrative proceeding related to fraud, extortion, bribery, bid rigging, embezzlement, misrepresentation or anti-trust; and
(5) been, and are not currently, the subject of a criminal investigation by any federal, state or local prosecuting or investigative agency or

civil anti-trust investigation by any federal, state, or local prosecuting or investigative agency.

(ii) Contractor Explanation. If the Contractor cannot make the representations and warranties set forth above at the time of its submission of its bid or proposal or if this contract is awarded on a non-bid basis at the time of the execution of the contract, the Contractor shall submit a written explanation outlining the reasons why it cannot make those representations and warranties. The Commonwealth may, based on its evaluation of the explanation provided, determine whether it is in the Commonwealth's best interest to execute the contract.

(iii) Further Representations. By submitting any bills, invoices, or requests for payment pursuant to this contract, the Contractor further represents that it has not violated any of these Contractor Integrity Provisions during the term of the contract.

(iv) Notice. The Contractor shall immediately notify the Commonwealth, in writing, if at any time during the term of the contract it becomes aware of any event that would cause the Contractor's certification or explanation to change. The Contractor acknowledges that the Commonwealth may, in its sole discretion, terminate the contract for cause if it learns that any of the certifications made in these provisions are currently false or misleading due to intervening factual circumstances or were false or misleading or should have been known to be false or misleading when entering into the contract.

(c) Contractor Responsibilities. During the term of this contract, the Contractor shall:

(i) maintain the highest standards of honesty and integrity.

(ii) take no action in violation of any applicable laws, regulations, or other requirements applicable to the Contractor that govern Commonwealth contracting and procurement.

(iii) establish and implement a written business integrity policy that includes, at a minimum, the requirements of these provisions as they relate to the Contractor's activity with the Commonwealth and Commonwealth employees and ensure that its employees comply with the policy.

(iv) not accept, agree to give, offer, confer, agree to confer, or promise to confer, directly or indirectly, any gratuity or pecuniary benefit to any person, or to influence or attempt to influence any person in violation of any federal or state law, regulation, executive order, statement of policy, management directive, or bulletin applicable to the provision of goods or services under this contract.

(v) not have a financial interest in any other contractor, subcontractor, or supplier providing services, labor, or material under this contract, unless the financial interest is disclosed to the Commonwealth in writing and the Commonwealth consents to Contractor's financial interest. The Contractor must disclose the financial interest to the Commonwealth at the time of bid or proposal submission, or if no bids or proposals are solicited, no later than the date the Contractor signs the contract. The Commonwealth shall be deemed to have consented if the required disclosure is received and all of the required Commonwealth signatures are affixed.

(vi) comply with the requirements of the Lobbying Disclosure Act (65 Pa.C.S. §13A01 et seq.) regardless of the method of award.

(vii) comply with the requirements of Section 1641 of the Pennsylvania Election Code (25 P.S. §3260a) if this contract was awarded on a Non-bid Basis.

(viii) immediately notify the Commonwealth contracting officer or the Office of the State Inspector General, in writing, when the Contractor has reason to believe that any breach of ethical standards as set forth in law, the Governor's Code of Conduct, or these Contractor Integrity Provisions has occurred or may occur, including, but not limited to, contact by a Commonwealth officer or employee, which, if acted upon, would violate the ethical standards.

(d) <u>Investigations</u>. If a State Inspector General investigation is initiated, the Contractor shall:

(i) reimburse the Commonwealth for the reasonable costs of investigation incurred by the Office of the State Inspector General for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the Commonwealth that results in the suspension or debarment of the Contractor. The Contractor shall not be responsible for investigative costs for investigations that do not result in the Contractor's suspension or debarment.

(ii) cooperate with the Office of the State Inspector General in its investigation of any alleged Commonwealth agency or employee breach of ethical standards and any alleged Contractor non-compliance with these Contractor Integrity Provisions and make identified Contractor employees available for interviews at reasonable times and places.

(iii) upon the inquiry or request of an Inspector General, provide, or if appropriate, make promptly available for inspection or copying, any information of any type or form deemed relevant by the Office of the State Inspector General to Contractor's integrity and compliance with these provisions. This information may include, but is not be limited to, Contractor's business or financial records, documents or files of any type or form that refer to or concern this contract.

(e) Termination. For violation of any of these Contractor Integrity Provisions, the Commonwealth may terminate this and any other contract with the Contractor, claim liquidated damages in an amount equal to the value of anything received in breach of these Contractor Integrity provisions, claim damages for all additional costs and expenses incurred in obtaining another contractor to complete performance under this contract, and debar and suspend the Contractor from doing business with the Commonwealth. These rights and remedies are cumulative, and the use or non-use of any one does not preclude the use of all or any other. These rights and remedies are in addition to those the Commonwealth may have under law, statute, regulation, or contract.

(f) Subcontracts. The Contractor shall include these Contractor Integrity Provisions in its contracts with all subcontractors providing goods or services under this contract. The incorporation of this provision in the Contractor's subcontracts does not create privity of contract between the Commonwealth and any subcontractor, and no third-party beneficiaries are created by the inclusion of these provisions. If the Contractor becomes aware of a subcontractor's violation of these provisions, the Contractor shall use its best efforts to ensure the subcontractor's compliance with these provisions.

62. ASSIGNMENT OF RIGHTS UNDER THE ANTITRUST LAWS.

The Contractor and the Commonwealth recognize that in actual economic practice, overcharges by Contractor's suppliers resulting from violations of state and federal antitrust laws are in fact borne by the Commonwealth. As part of the consideration for the award of this Contract, and intending to be legally bound, the Contractor assigns to the Commonwealth all rights, title, and interest in and to any claims Contractor now has or may hereafter acquire under state and federal antitrust laws relating to the goods and services which are subject to this Contract.

63. WARRANTIES.

Except as otherwise set forth in the Contract, the Contractor warrants that the Services, Supplies and Developed Works will conform in all material respects to the functional specifications for the Services, Supplies and Developed Works and/or the requirements of the Contract. The warranty period for the Services, Supplies and Developed Works shall be **90 days** from final acceptance. If third-party Services, Supplies or Developed Works are subject to a warranty that exceeds **90 days** from final acceptance, the longer warranty period shall apply. The Contractor shall correct any non-conformity within the warranty period specified herein.

(a) Disruption. The Contractor hereby represents and warrants to the Commonwealth that the Contractor will not intentionally cause, or intentionally take any action that causes a disruption of the Commonwealth's operations.

(b) Nonconformity. In the event of any nonconformity with the foregoing warranties, the Commonwealth will provide written notification of such nonconformity to the Contractor and the Contractor, at no cost to the Commonwealth, shall within **ten days'** notice of the nonconformity, commence work to remedy the nonconformity and shall work diligently, at no charge to the Commonwealth, until such time as the deliverable conforms, in all material respects, to the Service requirements and/or the functional specifications of the Developed Works set forth in this Contract. The Contractor shall have no obligation with respect to nonconformities arising out of:

(i) Modifications to Developed Works made by the Commonwealth;

(ii) Use of the Developed Works not in accordance with the documentation or specifications applicable thereto;

(iii) Failure by the Commonwealth to implement any corrections or enhancements made available by the Contractor;

(iv) Combination of the Developed Works with any items not supplied or approved by the Contractor; or

(v) Failure of any software licensed under a separate license agreement to conform to its specifications or documentation.

(c) Industry standards. The Contractor hereby represents and warrants to the Commonwealth that the Services shall be performed in accordance with industry standards using the utmost care and skill.

(d) Right to perform. The Contractor hereby represents and warrants to the Commonwealth that the Contractor has the necessary legal rights, including licenses to third party products, tools or materials, to perform the Services and deliver the Developed Works under this Contract.

(e) Sole warranties. THE FOREGOING EXPRESS WARRANTIES ARE THE CONTRACTOR'S SOLE AND EXCLUSIVE WARRANTIES AND NO OTHER WARRANTIES, EXPRESS OR IMPLIED, SHALL APPLY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

64. LIQUIDATED DAMAGES.

RESERVED

65. SERVICE LEVELS.

(a) The Contractor shall comply with the procedures and requirements of the Service Level Agreements, if any, which are made part of this Contract.

(b) Where there are expressly defined Service Levels, Contractor shall measure and report its performance against these standards on at least a monthly basis, except as may otherwise be agreed between the parties. Regardless of the presence or absence of expressly defined Service Levels, any failure to adequately or timely perform a Service may result in consequences under this Contract, up to and including Contract termination.

(c) The Commonwealth's acceptance of any financial credit incurred by the Contractor in favor of the Commonwealth for a Service Level default ("Service Level Credit") shall not bar or impair Commonwealth's rights and remedies in respect of the failure or root cause as set forth elsewhere in this Contract, including without limitation other claims for injunctive relief and termination rights; provided however, Service Level Credits paid would be credited against any such claims for damages.

66. FORCE MAJEURE.

(a) Neither party will incur any liability to the other if its performance of any obligation under this Contract is prevented or delayed by causes beyond its control and without the fault or negligence of either party. Causes beyond a party's control may include, but are not limited to, acts of God or war, changes in controlling law, regulations, orders or the requirements of any governmental entity, severe weather conditions, civil disorders, natural disasters, fire, epidemics and quarantines, general strikes throughout the trade, and freight embargoes.

(b) The Contractor shall notify the Commonwealth orally within **five days** and in writing within **ten days** of the date on which the Contractor becomes aware, or should have reasonably become aware, that such cause would prevent or delay its performance. Such notification shall (i) describe fully such cause(s) and its effect on performance, (ii) state whether performance under the contract is prevented or delayed and (iii) if performance is delayed, state a reasonable estimate of the duration of the delay. The Contractor shall have the burden of proving that such cause(s) delayed or prevented its performance despite its diligent efforts to perform and shall produce such supporting documentation as the Commonwealth may reasonably request. After receipt of such notification, the Commonwealth may elect to cancel the Contract, or to extend the time for performance as reasonably necessary to compensate for the Contractor's delay.

(c) In the event of a declared emergency by competent governmental authorities, the Commonwealth by notice to the Contractor, may suspend all or a portion of the Contract.

67. PUBLICITY/ADVERTISEMENT.

The Contractor shall not issue news releases, internet postings, advertisements, endorsements, or any other public communication without prior written approval of the Commonwealth, and then only in coordination with the Commonwealth. This includes the use of any trademark or logo.

68. TERMINATION ASSISTANCE.

(a) Upon the Commonwealth's request, Contractor shall provide termination assistance services (Termination Assistance Services) directly to the Commonwealth, or to any vendor designated by the Commonwealth. The Commonwealth may request termination assistance from the Contractor upon full or partial termination of the Contract and/or upon the expiration of the Contract term, including any renewal periods. Contractor shall take all necessary and appropriate actions to accomplish a complete, timely and seamless transition of any Services from Contractor to the Commonwealth, or to any vendor designated by the Commonwealth, without material interruption of or material adverse impact on the Services. Contractor shall cooperate with the Commonwealth and any new contractor and otherwise promptly take all steps required or reasonably requested to assist the Commonwealth in effecting a complete and timely transition of any Services.

(b) Such Termination Assistance Services shall first be rendered using resources included within the fees for the Services, provided that the use of such resources shall not adversely impact the level of service provided to the Commonwealth; then by resources already included within the fees for the Services, to the extent that the Commonwealth permits the level of service to be relaxed; and finally, using additional resources at costs determined by the Parties via **Section 27, Changes**.

69. NOTICE.

Any written notice to any party under this Contract shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

70. RIGHT-TO-KNOW LAW.

(a) Applicability. The Pennsylvania Right-to-Know Law, 65 P.S. §§ 67.101-3104, ("RTKL") applies to this contract.

(b) Contractor Assistance. If the Commonwealth needs the Contractor's assistance in any matter arising out of the RTKL related to this contract, the Commonwealth shall notify the Contractor that it requires the Contractor's assistance, and the Contractor shall provide to the Commonwealth:

(i) access to, and copies of, any document or information in the Contractor's possession (Requested Information) arising out of this contract that the Commonwealth reasonably believes is a public record under the RTKL, within ten calendar days after receipt of written notification; and

(ii) any other assistance as the Commonwealth may reasonably request, in order to comply with the RTKL with respect to this contract.

(c) Trade Secret or Confidential Proprietary Information. If the Contractor considers the Requested Information to include a Trade Secret or Confidential Proprietary Information, as those terms are defined by the RTKL, or other information that the Contractor considers exempt from production under the RTKL, the Contractor shall notify the Commonwealth and provide, within seven calendar days of receipt of the written notice a written statement, signed by a representative of the Contractor, that explains why the requested material is exempt from public disclosure under the RTKL. If the Commonwealth determines that the Requested Information is clearly not exempt from disclosure, the Contractor shall provide the Requested Information to the Commonwealth within five business days of receipt of written notice of the Commonwealth's determination.

(d) Reimbursement.

(i) Commonwealth Reimbursement. If the Contractor fails to provide the Requested Information and the Commonwealth is ordered to produce the Requested Information, the Contractor shall reimburse the Commonwealth for any damages, penalties, or costs that the Commonwealth may incur as a result of the Contractor's failure, including any statutory damages assessed against the Commonwealth.

(ii) Contractor Reimbursement. The Commonwealth will reimburse the Contractor for any costs that the Contractor incurs as a direct result of complying with these provisions only to the extent allowed under the fee schedule established by the Office of Open Records or as otherwise provided by the RTKL.

(e) Challenges of Commonwealth Release. The Contractor may file a legal challenge to any Commonwealth decision to release a record to the public with the Office of Open Records, or in the Pennsylvania Courts, however, the Contractor shall reimburse the Commonwealth for any legal expenses incurred by the Commonwealth as a result of the challenge, including any damages, penalties or costs that the Commonwealth may incur as a result of the Contractor's legal challenge, regardless of the outcome.

(f) Waiver. As between the parties, the Contractor waives all rights or remedies that may be available to it as a result of the Commonwealth's disclosure of Requested Information pursuant to the RTKL.

(g) Survival. The Contractor's obligations contained in this Section survive the termination or expiration of this contract.

71. APPLICABLE LAW AND FORUM.

This contract is governed by and must be interpreted and enforced in accordance with the laws of the Commonwealth of Pennsylvania (without regard to any conflict of laws provisions) and the decisions of the Pennsylvania courts. The Contractor consents to the jurisdiction of any court of the Commonwealth of Pennsylvania and any federal courts in Pennsylvania, and waives any claim or defense that such forum is not convenient or proper. Any Pennsylvania court or tribunal has in personam jurisdiction over the Contractor, and the Contractor consents to service of process in any manner authorized by Pennsylvania law. This provision may not be interpreted as a waiver or limitation of the Commonwealth's rights or defenses.

72. CONTROLLING TERMS AND CONDITIONS.

The terms and conditions of this Contract shall be the exclusive terms of agreement between the Contractor and the Commonwealth. Other terms and conditions or additional terms and conditions included or referenced in the Contractor's website, quotations, invoices, business forms, click-through agreements, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Contractor, and not binding on the Commonwealth.

73. POST-CONSUMER RECYCLED CONTENT; RECYCLED CONTENT ENFORCEMENT.

Except as specifically waived by the Department of General Services in writing, any products which are provided to the Commonwealth as a part of the performance of the Contract must meet the minimum percentage levels for total recycled content as specified by the Environmental Protection Agency in its Comprehensive Procurement Guidelines, which can be found at https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program.

The Contractor may be required, after delivery of the Contract item(s), to provide the Commonwealth with documentary evidence that the item(s) was in fact produced with the required minimum percentage of post-consumer and recovered material content.

74. WORKER PROTECTION AND INVESTMENT.

(a) The Contractor shall comply with all applicable Pennsylvania state labor laws and worker safety laws including, but not limited to, the following:

(i) Construction Workplace Misclassification Act;

(ii) Employment of Minors Child Labor Act;

(iii) Minimum Wage Act;

(iv) Prevailing Wage Act;

(v) Equal Pay Law;

(vi) Employer to Pay Employment Medical Examination Fee Act;

(vii) Seasonal Farm Labor Act;

(viii) Wage Payment and Collection Law;

(ix) Industrial Homework Law;

(x) Construction Industry Employee Verification Act;

(xi) Act 102: Prohibition on Excessive Overtime in Healthcare;

(xii) Apprenticeship and Training Act; and

(xiii) Inspection of Employment Records Law.

75. SURVIVAL.

The following Sections and any right or obligation of the parties in this Contract which, by its express terms or nature and context is intended to survive termination or expiration of this Contract, will survive any such termination or expiration shall survive the expiration or termination of the Contract.

(a) Section 11 (Order of Precedence);
(b) Section 30 (Contract Controversies);
(c) Section 31 (Confidentiality, Privacy and Compliance);
(d) Section 33 (Data Breach or Loss);
(e) Section 37 (Taxes-Federal, State and Local);
(f) Section 38 (Limitation of Liability);
(g) Section 39 (Indemnification);
(h) Section 41 (Virus, Malicious, Mischievous or Destructive Programming);
(i) Section 42 (Patent, Copyright, Trademark and Trade Secret Protection);
(j) Section 45 (Use of Commonwealth Property);
(k) Section 46 (Ownership of Developed Works);
(l) Section 47 (Source Code and Escrow Items Obligations);
(m) Section 48 (Contractor Hosted Security, Location, Status and Disposition Of Data);
(n) Section 49 (Publication Rights and/or Copyrights);
(o) Section 52 (Compliance with Laws);
(p) Section 54 (Examination of Records);

(q) Section 55 (Single Audit Act of 1984);
(r) Section 56 (Agency-Specific Sensitive and Confidential Commonwealth Data (If Applicable));
(s) Section 63 (Warranties);
(t) Section 67 (Publicity/Advertisement);
(u) Section 69 (Notice);
(v) Section 70 (Right-to-Know-Law);
(w) Section 71 (Applicable Law and Forum); and
(x) Section 75 (Survival).

EXHIBIT A

RESERVED.

EXHIBIT B

Requirements for Non-Commonwealth Hosted Applications/Services

The purpose of this Attachment is to define requirements for business or technology solutions and services procured by the Commonwealth that are hosted within the Service Organization (Contractor's) or its Subservice Organization(s) (subcontractors) managed infrastructure. Any reference to Contractor below applies to Contractor and its subcontractors.

A. Hosting Requirements

1. The Contractor shall supply and maintain all hosting equipment (hardware and software) required for the delivery of the computing services.

2. The Contractor shall provide secure access to users leveraging the principle of least privilege and delegating administration to the Commonwealth where possible.

3. The Contractor shall use commercially reasonable resources and efforts to maintain adequate network bandwidth and server capacity to meet expected service levels.

4. The Contractor shall maintain all components of the Contractor hosted solution with commercially reasonable support and replace as necessary to maintain compliance.

5. The Contractor shall monitor, prevent, and deter unauthorized system access. The Contractor shall use all commercially reasonable methods to confirm suspected breaches. In the event of any impermissible disclosure, unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. The Contractor shall provide the Commonwealth with any requested logs, reports, and other information concerning unauthorized access or disclosure of Commonwealth data, including any mitigation efforts by Contractor. Any such information provided by Contractor shall be treated as confidential. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Contractor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth within **one hour** of when the Contractor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

6. In the event the Contractor is not in compliance with **Section B System and Organization Controls (SOC) Reporting Requirements** relating to the hosted system's data center locations and security architecture, the Contractor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and with

at least **ten business days'** notice, to review the hosted system's data center locations and security architecture.

7. The Contractor's employees or subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.

8. The Contractor shall house all servers and equipment in an operational environment that meets industry standards including, but not limited to, climate control, fire and security hazard detection and response, electrical needs, and physical security.

9. The Contractor shall examine applicable system and error logs, which should include, but not be limited to, security events. Such logs shall be examined on a continual basis, at least daily, to minimize and predict system problems and initiate appropriate action.

10. The Contractor shall update and patch all applicable systems and third-party software security configurations to reduce security risk in alignment with industry best practices beginning prior to service release and on an ongoing basis.

11. During the term of the contract, the Contractor shall provide or make available all Commonwealth data to the Commonwealth, at no cost and upon request in a format and method agreeable to both parties. If the parties are unable to reach an agreement regarding format or method, data shall be provided in an industry standard format and method.

B. System and Organization Controls (SOC) Reporting Requirements

1. Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Contractor shall, and shall require its subcontractors to, engage, on an annual basis, a CPA certified third-party auditing firm to conduct the following, as applicable:

   (i) a SOC 1 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that process Commonwealth financial transactions; and

   (ii) a SOC 2 Type II report with respect to controls used by the Contractor relevant to internal and external procedures and systems that access, process, host or contain Commonwealth Data designated as Class "C" Classified Records or Closed Records, as defined in the Commonwealth's Data Classification Policy, or in compliance with mandates by federal or state audit requirements and/or policy.

The Contractor shall receive and review their subcontractor's relevant SOC reports, and the Contractor shall provide the Commonwealth with a Letter of Attestation that includes an analysis of their subcontractor's SOC report.

2. Unless otherwise agreed to in writing by the Commonwealth, the Contractor's SOC Report(s) shall be provided upon contract execution and annually thereafter. While it is preferable that SOC Reports coincide with Pennsylvania's fiscal year (July 1 through June 30), SOC Reports, at the very least, must cover at least **six consecutive months** of Pennsylvania's fiscal year.

3. SOC 2 Type II reports shall address the following:

    (i) Security of Information and Systems;
    (ii) Availability of Information and Systems;
    (iii) Processing Integrity;
    (iv) Confidentiality; and
    (v) Privacy.

4. At the request of the Commonwealth and at Contractor's expense, the Contractor shall, and shall require its subcontractors, as applicable, to complete a SOC for Cybersecurity audit in the event:

    (i) Reoccurring findings in any SOC report required by subsection 1 above; or

    (ii) A cybersecurity incident or breach that impacts the Commonwealth has occurred and was not handled in accordance with Contractor's Incident Response Plan (IRP) including, but not limited to, providing timely notice to the Commonwealth as required by Contract or applicable law; or

    (iii) As agreed upon by the parties.

    The SOC for Cybersecurity report shall detail the controls used by the Contractor or its subcontractor setting forth the description and effectiveness of the Contractor's or subcontractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

    The Contractor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings within **60 days** of its completion.

5. Additional standards, certifications or audits as required by law shall be supported by Contractor as mutually agreed upon in writing by the parties.

6. The Contractor shall adhere to the then current American Institute of Certified Public Accountants (AICPA) audit standards. The Contractor acknowledges that the AICPA guidance may be updated during the Term of this Contract, and the

Contractor shall comply with such updates, which shall be reflected in the next annual SOC report.

7. In the event an audit reveals any non-conformity within Contractor's SOC Reports, the Contractor shall provide the Commonwealth, within **45 days** of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity that is identified within the SOC report, including any subcontractor's SOC report. The corrective action plan shall provide, in detail:

   (i) clear responsibilities of the personnel designated to resolve the non-conformity;
   (ii) the remedial action to be taken by the Contractor or its subcontractor(s);
   (iii) the dates when each remedial action is to be implemented; and
   (iv) a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).

8. The Commonwealth may in its sole discretion agree, in writing, to accept alternative security report in lieu of a SOC report.

C. Security Requirements

1. The Contractor shall conduct a third-party independent security/vulnerability assessment at its own expense no less frequently than on an annual basis.

2. The Contractor shall provide, at minimum, an executive summary of vulnerability assessment results to the Commonwealth upon request. Summary shall include, at minimum, scan date, identified vulnerabilities, severity classification, and remediation status.

3. The Contractor shall remediate any security/vulnerability assessment findings to align with the industry standards.

4. The Contractor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

5. The Contractor shall use industry best practices to secure access to public web interfaces, which shall include, but is not limited to, web application firewall (WAF) for services that handle non-public Commonwealth records.

6. The Contractor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.

7. The Contractor shall use industry best practices, such as those outlined in NIST 800-83, to provide appropriate exploit and malware controls, on all servers, endpoints, and network components.

8. The Contractor shall provide access to provided systems and services and/or Commonwealth data only to staff located within CONUS (any of the Continental United States and Hawaii). Access shall be based on the principle of least privilege.

9. The Contractor shall provide the services using security technologies and techniques in accordance with industry best practices including, but not limited to, the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.

10. The Contractor shall provide the Commonwealth with access to audit logs with respect to the services being provided to the Commonwealth within 24 hours of a written request from the Commonwealth's Enterprise Information Security Office.

D. Data Protection

1. The Contractor shall only host, handle, and process data in physical locations within CONUS.

2. The Contractor shall use industry best practices to protect their operational systems with applicable anti-virus, intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.

3. The Contractor shall be solely responsible for applicable data storage required.

4. The Contractor shall encrypt all Commonwealth data in transit and at rest. The Contractor's method of data encryption shall meet or exceed National Institute Standards and Technology (NIST) encryption guidelines and standards in alignment with Commonwealth ITPs.

5. The Contractor shall take all commercially viable and appropriate measures to protect the data availability including, but not limited to, real-time replication, traditional backup, and/or georedundant storage of Commonwealth data in accordance with industry best practices and encryption techniques.

6. The Contractor shall have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Contractor-controlled or Contractor-owned electronic device.

7. The Contractor shall utilize a secured backup solution to prevent loss of data. Stored backups must be kept in an all-hazards protective storage environment at the primary location and any additional locations where the data is being maintained. All back up data and media shall be encrypted.

E. Adherence to Policy

1. The Contractor support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.

2. The Contractor shall abide by the Commonwealth's Information Technology Policies (https://www.pa.gov/agencies/oa/policies/it-policies) that are applicable to the products and services provided, as set forth within the responsibilities section of each ITP.

3. The Contractor shall comply with all pertinent federal and state regulations and laws, including but not limited to, data protections, data security, privacy, and data breach notification.

F. Closeout

When the purchase order's or other procurement document's term expires or terminates, and a new purchase order or other procurement document has not been issued by a Commonwealth Agency within **60 days** of expiration or termination, or at any other time at the written request of the Commonwealth, the Contractor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Contractor's possession or control. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth.

Upon confirmation that Commonwealth data is in possession or control of the Commonwealth, the Contractor shall ensure all residual user account(s) are promptly deleted or reset in the solution. The Contractor shall notify the Commonwealth within **ten business days** that all user account(s) have been deleted or reset.

EXHIBIT C

Sign-Off Document No. ____, under Agreement No. __________
Between
[Contractor____________________] and the Commonwealth of PA, [Agency]

[Contractor____________________] Agency-level Deployment

This document becomes, upon its execution by the signatories named below, a legally valid, binding part of Agreement No. _________ between the Commonwealth and ______ (Contractor), and is subject to the terms of that Agreement.

1. Scope of Deployment (need not be entire agency):

2. Nature of Data implicated or potentially implicated:

3. Agency Policies to which Contractor is subject (incorporated by reference):

4. Background checks (describe if necessary):

5. Additional requirements (describe with specificity):

6. Is Contractor a Business Associate (yes or no)?

If yes, the attached Business Associates Agreement, as completed by the Agency, is applicable and is hereby incorporated into this Sign-Off Document by reference.

Agency Contact Person Signature and Date: ____________________________________

[Contractor____________________]
Authorized Signatory and Date: ____

Contract No. 4400034320

PARTICIPATING ADDENDUM
UNDER
STATE OF UTAH COOPERATIVE CONTRACT
Utah Contract Number LS4983

This Participating Addendum ("Addendum") is entered into pursuant to the State of Utah Cooperative Contract, Contract Number LS4983 ("Utah Cooperative Contract"), between **Carahsoft Technology Corp.** ("Contractor") and the State of Utah Division of Purchasing ("Utah"). The parties to this Addendum hereby create a separate contract between the Contractor and the **Commonwealth of Pennsylvania** ("Commonwealth") acting through its **Department of General Services** ("DGS").

Utah, pursuant to law governing federal acquisitions, entered into the Utah Cooperative Contract with the Contractor, pursuant to which the Contractor provides various On-Premise and Cloud products and related services, including Software as a Service (SaaS), Infrastructure as Service (IaaS), and Platforms as a Service (PaaS), and related Services as described in the Utah Cooperative Contract; and

The Commonwealth of Pennsylvania desires to participate in the Utah Cooperative Contract as an additional contracting party under the Utah Cooperative Contract.

DGS is authorized under Section 1902 and 1908 of the Commonwealth Procurement Code, 62 Pa.C.S. §§1902, 1908, to undertake and make this type of contractual arrangement on behalf of the Commonwealth.

DGS and the Contractor, intending to be legally, agree as follows:

1. **Recitals.** The recitals set forth above are incorporated by reference as a material part of this Addendum.

2. **Term and Termination.** This Addendum shall become effective on the date the Commonwealth sends the fully executed and approved Addendum to the Contractor (the "Effective Date") and shall extend for an initial term of five years, with five one-year renewal options to be exercised at the discretion of the Commonwealth by providing no less than 30 days prior written notice to the Contractor. This Addendum shall terminate or expire upon the earlier of (a) expiration of the then-current term if the Commonwealth has not elected to renew, (B) termination of the Utah Cooperative Contract, or (c) termination of this Addendum in accordance with its terms or the terms of the Utah Cooperative Contract.

3. **Addendum Terms.** DGS and the Contractor agree to be bound to the IT Contract Terms and Conditions attached hereto as Exhibit A and made part of this Addendum.

4. **Utah Cooperative Contract Terms.** DGS and the Contractor agree to be bound by the prices, terms and conditions stated in the Utah Cooperative Contract, which is incorporated into and made a part of this Addendum as **Exhibit B**.

5. **Supplies and Services Available to Procure.** The Commonwealth may procure any of those items and/or services specified in Attachment B, Scope of Work, to the Utah Cooperative Contract. Any item and/or service provided by the Contractor through the Utah Cooperative Contract but not listed above may be added or substituted to this Addendum at the sole discretion of DGS.

6. **Maintenance.** Unless prohibited by the Utah Cooperative Contract, Contractor may provide software maintenance ("Maintenance") to the Commonwealth through this Addendum. Contractor may provide Maintenance to the Commonwealth beyond the expiration date of the Utah Cooperative Contract if a purchase order for such services is executed prior to the expiration date of this Addendum and the Utah Cooperative Contract.

7. **End-User Software License Agreement**. To the extent that End-User Software License Agreements are required to use items and/or services from the Utah Cooperative Contract, the Commonwealth shall enter into a separate agreement with the appropriate Licensor.

8. **Price Quote**. Purchase Orders issued pursuant to this Addendum must include a price quote and reference any applicable End-User Software License Agreement executed between the parties. In the event of inconsistencies between this Addendum and the End-User Software License Agreement, the parties agree that End-User Software License Agreement prevails only with respect to the specific subject matter addressed therein.

9. **Order of Precedence.** To the extent that there is a conflict, the order of precedence shall be as follows:

    a. this Addendum;
    b. the IT Contract Terms and Conditions attached as Exhibit A; and then
    c. the Utah Cooperative Contract attached as Exhibit B.

10. **Commonwealth of Pennsylvania Addendum Participants.** This Addendum may be used by all "Commonwealth agencies" as that term is defined in Section 103 of the *Commonwealth Procurement Code*, 62 Pa. C.S. § 103, and by all "local public procurement units", as that term is defined in Section 1901 of the *Commonwealth Procurement Code*, 62 Pa. C.S. § 1901.

11. **Reporting Requirements**

    (a) <u>Quarterly Reporting</u>**.** The Contractor shall provide to the Commonwealth's primary contact a quarterly report detailing purchasing volume by the Commonwealth and its using agencies. The report shall also include all COSTARS purchases. A consistent reporting mechanism will be required and shall include, but not be limited to:

(1) A Summary Report of purchases by each Commonwealth agency (item description, item number, serial number, subtotals, and totals), including the delivery order history indicating the receipt date of the purchase order, and the delivery date of equipment.

(2) A Performance Report indicating average delivery time for equipment, percentage of orders that were shipped incorrectly, failure rates ('dead on arrival'), and percentage of delivery orders resulting in backorder items.

(3) Usage reports as defined the Commonwealth.

(4) A Call-Tracking Report for warranty/maintenance support, which shall include:
- Date of initial call, requesting agency, contact person, and nature of call
- Date of initial Contractor response
- Date and brief explanation of problem closure

(5) A Customer Satisfaction Report detailing Contractor performance in the areas of quality assurance, accuracy of equipment shipped, professionalism, flexibility, competence, timeliness of delivery and response to questions. Contractor shall initiate customer satisfaction surveys indicating Contractor performance. The Commonwealth will determine the format and delivery mode of the survey.

(b) Report Requirements:

(1) *Report Due Date***:** The Contractor shall provide all reports to the Commonwealth no later than ten (10) days after the end of the applicable reporting period (month or quarter).

(2) *Report specifications*: All reports shall be in Microsoft Excel format. Download all requested reports to one Excel file. Use tabs to define each report. Ensure to label file, report, tabs, and cells correctly. Ensure Commonwealth of Pennsylvania and COSTARS (if applicable) data is segregated and labeled correctly. Reports are to be sent to the Department of General Services.

(c) Reports may be added or deleted as required by the Department of General Services.

12. **Iran Free Procurement Certification.** Prior to entering a contract worth at least $1,000,000 or more with a Commonwealth entity, a Contractor must: a) certify it is not on the current list of persons engaged in investment activities in Iran created by the DGS pursuant to Section 3503 of the Procurement Code and is eligible to contract with the Commonwealth under Sections 3501-3506 of the Procurement Code; or b) demonstrate it has received an exception from the certification requirement for that solicitation or contract pursuant to Section 3503(e). Contractor must complete and return the Iran Free Procurement Certification form.

13. **Worker Protection and Investment Certification.** Pursuant to Executive Order 2021-06, Worker Protection and Investment (October 21, 2021), the Commonwealth is responsible

for ensuring that every Pennsylvania worker has a safe and healthy work environment, and the protections afforded them through labor laws. To that end, contractors and grantees of the Commonwealth must certify that they are in compliance with all applicable Pennsylvania state labor and workforce safety laws. Such certification shall be made through the Worker Protection and Investment Certification Form (BOP-2201). Contractor must complete and return the Worker Protection and Investment Certification form.

14. **Lobbying Certifications and Disclosure**. With respect to an award of a federal contract, grant, or cooperative agreement exceeding $100,000 or an award of a federal loan or a commitment providing for the United States to insure or guarantee a loan exceeding $150,000 all recipients must certify that they will not use federal funds for lobbying and must disclose the use of non-federal funds for lobbying by filing required documentation. The Contactor must complete and return the Lobbying Certification Form and the Disclosure of Lobbying Activities Form. Commonwealth agencies will not contract with outside firms or individuals to perform lobbying services, regardless of the source of funds.

15. **Primary Contact; Notice**. The primary contacts for this Addendum, as well as the recipients of any written notices shall be the individuals identified below or such other individuals as may be identified from time to time in a Notice sent by a designating party to the other parties set forth below, except that a Purchase Order issued pursuant to this Addendum will identify the Commonwealth Contact Person identified in the Purchase Order.

    The Commonwealth's primary contact, Issuing Officer and Contracting Officer for this Addendum is as follows:

    Scott Cropper
    Department of General Services
    1802 Herr Street
    Harrisburg, PA 17103
    (717) 346-3819
    scropper@pa.gov

    The Contractor's primary contact for this Addendum, including and notice is as follows:

    Mariah Edwards
    Carahsoft Technology Group
    11493 Sunset Hills Road, Suite 100
    Reston, VA 20190
    Mariah.edwards@carahsoft.com

    All notices, approvals, consents and requests pursuant to this Addendum shall be sent to the parties at their respective addresses listed above, or to such other address as may be designated from time to time by the parties without the need to further amend the Addendum: Changes to the Contractor's contact information, company name, legal address, payment address, tax identification number, authorized signatories, or EFT information must be promptly reported via email to the Contracting Officer, and updated in the PA Supplier Portal, https://pasupplierportal.state.pa.us/irj/portal/anonymous. In some cases, additional paperwork will be required to effect the change.

16. **Audit Provisions.** The Commonwealth, excluding information protected by privacy laws, shall have the right, with at least one business week's notice and during regular business hours, and at Contractor's headquarters in Sec. 15, to audit the books, documents, and records of the Contractor to the extent that the books, documents, and records relate specifically to pricing data for this Addendum or order. The Contractor agrees to maintain records that will support the prices charged for this Participating Addendum or any order. The Contract or shall preserve books, documents, and records that relate to pricing data for this Participating Addendum or any order for a period of **three years** from date of final payment.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

The parties, through their authorized representatives, have signed this Addendum the day and year first above written.

CARAHSOFT TECHNOLOGY CORP.

Signature: Madeline Hall

Print Name: Madeline Hall

Date: 7/20/2026

Title: Senior Contracts Administrator

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF GENERAL SERVICES

By: Signature To be obtained electronically

Deputy Secretary Date

APPROVED:

Signature To be obtained electronically

Comptroller Date

APPROVED AS TO FORM AND LEGALITY:

Signature To be obtained electronically

Office of Chief Counsel Date

Signature To be obtained electronically

Office of General Counsel Date

Signature To be obtained electronically

Office of Attorney General Date

Contract # LS4983

STATE OF UTAH COOPERATIVE CONTRACT

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

Carahsoft Technology Corporation
Name
11493 Sunset Hills Road, Suite 100
Address
Reston VA 20190
City State Zip

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

Contact Person Beth Drake Phone #703-889-9734 Email NASPO@carahsoft.com
Vendor # VC0000116540 Commodity Code #92005

2. CONTRACT PORTFOLIO NAME: Cloud and Software Solutions

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

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

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

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

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this Contract.
   b. Utah State Procurement Code, Procurement Rules, the Solicitation, and Contractor's response to the Solicitation.

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:
Robert Moore
A8FDBA7CEA5A4BC...

Contractor's Signature	Print Name	Title	Date
	Robert Moore	Vice President	11/13/2025

STATE

DocuSigned by:
C38BE9DAC528424...

Director, Division of Purchasing	Date
	11/14/2025

ATTACHMENT A

NASPO VALUEPOINT MASTER AGREEMENT TERMS AND CONDITIONS

I. Definitions

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

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

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

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

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

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

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

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

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

1.8 **End User Agreement** means any agreement or additional terms and conditions that

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

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

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

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

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

1.12 **Intellectual Property** means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

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

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

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

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

1.17 **NASPO ValuePoint** is a division of the National Association of State Procurement Officials ("NASPO"), a 501(c)(3) corporation. NASPO ValuePoint facilitates administration of the NASPO cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (*i.e.*, colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports, as well as other contract administration functions as assigned by the Lead State.

1.18 **Non-Public Data** means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

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

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

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

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

1.23 **Personal Data** means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or

description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person. Federal Tax Information (FTI) as defined by the federal government Internal Revenue Service Publication 1075 (as updated, replaced, or amended over time).

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

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

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

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

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

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

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

1.31 **Subcontractor** includes contractors, manufacturers, distributors, suppliers, or consultants, at any tier, that are under the direct or indirect control or responsibility of

Contractor, including a person or entity that is, or will be, providing Product or Products and Services pursuant to this Master Agreement.

II. Term of Master Agreement

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

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

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

III. Order of Precedence

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

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

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

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

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

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

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

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

III.2 Conflict. These documents will be read to be consistent and complementary. Any conflict among these documents will be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

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

IV. Participants and Scope

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

IV.2 Applicability of Master Agreement. NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum, subject to Section III. For the purposes of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (*e.g.*, purchase order or contract) used by the Purchasing Entity to place the Order.

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

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

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

IV.6 Participating Entities.

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

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

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

IV.6.1.3 Federally recognized tribes;

IV.6.1.4 Quasi-governmental entities; and

IV.6.1.5 Eligible non-profit organizations.

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

IV.7 Prohibition on Resale. Subject to any specific conditions included in the Solicitation or Contractor's proposal as accepted by the Lead State, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products purchased under this Master Agreement. Absent any such condition or explicit permission, this limitation does not prohibit: payments by employees of a Purchasing Entity for Products; sales of Products to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of Intellectual Property.

IV.8 Individual Customers. Except as may otherwise be agreed to by the Purchasing Entity and Contractor, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement and as the Participating Entity has in the Participating Addendum, including but not limited to any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

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

IV.10 No Representations. The Contractor shall not make any representations of NASPO ValuePoint, the Lead State, any Participating Entity, or any Purchasing Entity's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent.

V. NASPO ValuePoint Provisions

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

V.2 Administrative Fees

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

V.2.2 State Imposed Fees. Some states may require an additional fee be paid by Contractor directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee rate or amount, payment method, and schedule for such reports and payments will be incorporated into the applicable Participating Addendum. Unless agreed to in writing by the state, Contractor may not adjust the Master Agreement pricing to include the state fee for purchases made by Purchasing Entities within the jurisdiction of the state. No such agreement will affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by Purchasing Entities outside the jurisdiction of the state requesting the additional fee.

V.3 NASPO ValuePoint Summary and Detailed Usage Reports

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

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

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

V.3.4 Sales Data Crosswalks. Upon request by NASPO ValuePoint, Contractor shall provide to NASPO ValuePoint tables of customer and Product information and specific attributes thereof for the purpose of standardizing and analyzing reported Sales Data ("Crosswalks"). Customer Crosswalks must include a list of existing and potential Purchasing Entities and identify for each the appropriate customer type as defined by NASPO ValuePoint. Product Crosswalks must include Contractor's part number or SKU for each Product in Offeror's catalog and identify for each the appropriate Master Agreement category (and subcategory, if applicable), manufacturer part number, Product description, eight-digit UNSPSC Class Level commodity code, and (if applicable) EPEAT value and Energy Star rating. Crosswalk requirements and fields may be updated by NASPO ValuePoint with reasonable notice to Contractor and without amendment to this Master Agreement. Contractor shall work in good faith with NASPO ValuePoint to keep Crosswalks updated as Contractor's customer lists and Product catalog change.

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

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

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

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

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

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

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

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

V.5 NASPO ValuePoint eMarketPlace

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

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

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

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

V.5.5 Contractor is solely responsible for the accuracy, quality, and legality of Contractor's Content on the eMarketPlace. "Content" means all information that is generated, submitted, or maintained by Contractor or otherwise made available by Contractor on the eMarketPlace, including

Contractor catalogs. Contractor's Content shall comply with and accurately reflect the terms and pricing of this Master Agreement.

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

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

V.5.8 Lead State reserves the right to approve all pricing, catalogs, and information on the eMarketPlace. This catalog review right is solely for the benefit of the Lead State and Participating Entities, and the review and approval shall not waive the requirement that Products and Services be offered at prices required by the Master Agreement.

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

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

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

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

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

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

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

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

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

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

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

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

V.5.12.3 Detailed Product line item descriptions;

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

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

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

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

V.8 **Additional Agreement with NASPO.** Upon request by NASPO ValuePoint, awarded Contractor shall enter into a direct contractual relationship with NASPO

ValuePoint related to Contractor's obligations to NASPO ValuePoint under the terms of the Master Agreement, the terms of which shall be the same or similar (and not less favorable) than the terms set forth in the Master Agreement.

VI. Pricing, Payment & Leasing

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

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

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

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

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

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

VII. Ordering

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

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

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

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

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

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

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

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

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

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

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

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

VII.6.1 The services or supplies being delivered;

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

VII.6.3 A billing address;

VII.6.4 Purchasing Entity contact information;

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

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

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

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

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

VIII. Shipping and Delivery

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

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

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

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

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

IX. Inspection and Acceptance

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

IX.2 **Applicability.** Unless otherwise specified in the Master Agreement, Participating

Addendum, or ordering document, the terms of this Section IX will apply. This section is not intended to limit rights and remedies under the applicable commercial code.

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

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

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

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

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

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

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

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

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

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

X. Warranty

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

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

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

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

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

XI. Product Title

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

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

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

XII. Indemnification

XII.1 General Indemnification. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers and employees, from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property arising from any act, error, or omission of the Contractor, its employees or Subcontractors or volunteers, at any tier, relating to performance under this Master Agreement.

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

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

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

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

XII.2.1.3 reasonably required to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

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

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

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

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

XIII. Insurance

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

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

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

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

XIII.3.2 CLOUD MINIMUM INSURANCE COVERAGE:

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 to hold itself out as agent except as expressly set forth herein or as expressly set forth in an applicable Participating Addendum or Order.

XIV.6 Cancellation. Unless otherwise set forth herein, this Master Agreement may be canceled by either party upon sixty (60) days' written notice prior to the effective date of the cancellation. Further, any Participating Entity may cancel its participation upon thirty (30) days' written notice, unless otherwise limited or stated in the Participating Addendum. Cancellation may be in whole or in part. Any cancellation under this provision will not affect the rights and obligations attending Orders outstanding at the time of cancellation, including any right of a Purchasing Entity to indemnification by the Contractor, rights of payment for Products delivered and accepted, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit. Cancellation of the Master Agreement due to Contractor default may be immediate.

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

XIV.8 Defaults and Remedies

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

XIV.8.1.1 Nonperformance of contractual requirements;

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

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

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

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

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

XIV.8.3 If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and the Lead State shall have the right to exercise any or all of the following remedies:

XIV.8.3.1 Any remedy provided by law;

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

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

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

XIV.8.3.5 Suspension of Contractor's performance; and

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

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

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

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

XIV.11 No Waiver of Sovereign Immunity

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

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

XIV.12 Governing Law and Venue

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

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

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

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

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

Attachment A.1 – Software Publisher Terms and Conditions

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

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

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

1. Definitions:

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

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

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

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

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

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

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

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

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

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

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

a. The service provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with NIST SP 800- 53 (then current, or prior version compliant with the appropriate certification body's requirements) and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. Access to Security Logs and Reports:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

28. Termination and Suspension of Service:

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

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

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

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

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

d. The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established in the SOW.

e. The service provider shall securely dispose of all requested data in all forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

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

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

1. Definitions:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

28. Termination and Suspension of Service:

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

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

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

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

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

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

1. Definitions:

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

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

c. **d. Infrastructure-as-a-Service (IaaS):** The capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls). .

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. Access to Security Logs and Reports:

a. The service provider shall provide reports to the public jurisdiction directly related to the infrastructure that the service provider controls upon which the public jurisdiction account resides. Unless otherwise agreed to in the SLA or End User Agreement, the service provider shall provide the public jurisdiction a history of all API calls for the public jurisdiction's account. This report shall include the identity of the API caller, the date and time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the service provider. The report will be sufficient to enable the public jurisdiction to perform security analysis, resource change tracking and compliance auditing.

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

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

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

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

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

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

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

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

Review of control documentation by internal staff or 3PAOs

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

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

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

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

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

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

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

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

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

28. Termination and Suspension of Service:

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

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

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

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

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

Attachment A.2 – On-Premises Terms and Conditions

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

Attachment B
SCOPE OF WORK

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

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

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

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

I. Scope of Work Overview:

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

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

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

Definitions:

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

1. Definitions, Roles, and Responsibilities:

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Categorization of Risk

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

a. Low Risk Data

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

Low Impact levels are defined in FIPS 199 as follows:

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

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

b. Moderate Risk Data

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

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

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

c. High Risk Data

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

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

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

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

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

3. Service Models

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

Award Categories:

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

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

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

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

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

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

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

4. Deployment Models

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

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

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

II. NEW TECHNOLOGY

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

III. CATALOG UPDATES

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

At a minimum, Contractor's detailed catalog must identify the name and description of the Product offered, the Product provider's name, and the role of the Product provider under the Contract (e.g. Fulfilment Partner, Subcontractor, or Third-party Provider). Contractor catalog must list all Products and Services with SKUs (or some equivalent identifiers) and pricing. Pricing must demonstrate the correct contract price with the MSRP (or list price or equivalent if MSRP is not available), discount percentage, and Master Agreement price clearly listed.

Additionally, Contractor must provide a summary catalog document listing all the solutions' names and Products available on the Master Agreement, but without all the pricing, line items, and SKU details. This will help Participating Entities more easily see what is available in a much more accessible document than the full detailed catalog.

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

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

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

Attachment C Pricing Discounts and Schedule

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

Minimum Discount % Off MSRP	Software (Saas)	Infrastructure (Iaas)	Platform (Paas)	On-Premises	Value Added Services*
Direct Service Providers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	2%	2%	2%	2%	2%
Value-Added Resellers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	2%	2%	2%	2%	2%
Maximum Markup %	**Software (Saas)**	**Infrastructure (Iaas)**	**Platform (Paas)**	**On-Premises**	**Value Added Services***
Value-Added Resellers: Maximum Markup %	18%	18%	18%	18%	18%

Attachment D

Contractor’s Response to the Solicitation

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

Attachment E

End User Agreements

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

Attachment F: Third-party Provider Agreement (Template)

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

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

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

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

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

Lead State Approval:

Attachment G
IRS Publication 1075 Exhibit 7

Exhibit 7 Safeguarding Contract Language

I. PERFORMANCE

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

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

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

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

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

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

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

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

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

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

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

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

obligated to the agency under this contract.

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

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

II. CRIMINAL/CIVIL SANCTIONS

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

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

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

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

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

III. INSPECTION

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

IRAN FREE PROCUREMENT CERTIFICATION FORM

(Pennsylvania's Procurement Code Sections 3501-3506, 62 Pa.C.S. §§ 3501-3506)

To be eligible for an award of a contract with a Commonwealth entity for goods or services worth at least $1,000,000 or more, a vendor must either: a) certify it is **not** on the current list of persons engaged in investment activities in Iran created by the Pennsylvania Department of General Services ("DGS") pursuant to Section 3503 of the Procurement Code and is eligible to contract with the Commonwealth under Sections 3501-3506 of the Procurement Code; or b) demonstrate it has received an exception from the certification requirement for that solicitation or contract pursuant to Section 3503(e).

To comply with this requirement, please insert your vendor or financial institution name and complete **one** of the options below. Please note: Pennsylvania law establishes penalties for providing false certifications, including civil penalties equal to the greater of $250,000 or twice the amount of the contract for which the false certification was made; contract termination; and three-year ineligibility to bid on contracts. (Section 3503 of the Procurement Code.)

OPTION #1 - CERTIFICATION

I, the official named below, certify I am duly authorized to execute this certification on behalf of the vendor/financial institution identified below, and the vendor/financial institution identified below is **not** on the current list of persons engaged in investment activities in Iran created by DGS and is eligible to contract with the Commonwealth of Pennsylvania Sections 3501-3506 of the Procurement Code.

Vendor Name/Financial Institution (Printed) Carahsoft Technology Corp.	
By (Authorized Signature) Madeline Hall	
Printed Name and Title of Person Signing Madeline Hall, Contracts Manager	*Date Executed* 1/23/2026

OPTION #2 – EXEMPTION

Pursuant to Procurement Code Section 3503(e), DGS may permit a vendor/financial institution engaged in investment activities in Iran, on a case-by-case basis, to enter into a contract for goods and services.

If you have obtained a written exemption from the certification requirement, please fill out the information below, and attach the written documentation demonstrating the exemption approval.

Vendor Name/Financial Institution (Printed)	
By (Authorized Signature)	
Printed Name and Title of Person Signing	*Date Executed*

WORKER PROTECTION AND INVESTMENT CERTIFICATION FORM

A. Pursuant to Executive Order 2021-06, *Worker Protection and Investment* (October 21, 2021), the Commonwealth is responsible for ensuring that every worker in Pennsylvania has a safe and healthy work environment and the protections afforded them through labor laws. To that end, contractors and grantees of the Commonwealth must certify that they are in compliance with Pennsylvania's Unemployment Compensation Law, Workers' Compensation Law, and all applicable Pennsylvania state labor and workforce safety laws including, but not limited to:

1. Construction Workplace Misclassification Act
2. Employment of Minors Child Labor Act
3. Minimum Wage Act
4. Prevailing Wage Act
5. Equal Pay Law
6. Employer to Pay Employment Medical Examination Fee Act
7. Seasonal Farm Labor Act
8. Wage Payment and Collection Law
9. Industrial Homework Law
10. Construction Industry Employee Verification Act
11. Act 102: Prohibition on Excessive Overtime in Healthcare
12. Apprenticeship and Training Act
13. Inspection of Employment Records Law

B. Pennsylvania law establishes penalties for providing false certifications, including contract termination; and three-year ineligibility to bid on contracts under 62 Pa. C.S. § 531 (Debarment or suspension).

CERTIFICATION

I, the official named below, certify I am duly authorized to execute this certification on behalf of the contractor/grantee identified below, and certify that the contractor/grantee identified below is compliant with applicable Pennsylvania state labor and workplace safety laws, including, but not limited to, those listed in Paragraph A, above. I understand that I must report any change in the contractor/grantee's compliance status to the Purchasing Agency immediately. I further confirm and understand that this Certification is subject to the provisions and penalties of 18 Pa. C.S. § 4904 (Unsworn falsification to authorities).

Madeline Hall	1/23/2026
Signature	***Date***
Madeline Hall	
Name (Printed)	
Contracts Manager	
Title of Certifying Official (Printed)	
Carahsoft Technology Corp.	
Contractor/Grantee Name (Printed)	

pennsylvania
DEPARTMENT OF GENERAL SERVICES
BUREAU OF PROCUREMENT

LOBBYING CERTIFICATION FORM

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, Disclosure of Lobbying Activities, which can be found at:

http://www.whitehouse.gov/sites/default/files/omb/assets/omb/grants/sflllin.pdf

(3) The undersigned shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed under *Section 1352, Title 31, U. S. Code.* Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than **$100,000** for such failure.

SIGNATURE: Madeline Hall

TITLE: Contracts Manager DATE: 1/23/2026

BOP-1307
Revised 11/7/2013