

CLOUD AND SOFTWARE SOLUTIONS

Led by the State of Utah

Master Agreement #: **LS5021** (*hereinafter "Master Agreement"*)

Contractor: **SHI INTERNATIONAL CORP** (*hereinafter "Contractor"*)

Participating State: **STATE OF HAWAII** (*hereinafter "Participating State"*)

State of Hawaii, State Procurement Office (SPO) Vendor List Contract No. 26-13

This Addendum will add the State of Hawaii as a Participating State to purchase from the NASPO ValuePoint Master Agreement Number LS5021 with SHI International Corp.

1. Scope: This addendum covers the Cloud and Software Solutions led by the State of Utah for use by state agencies and other entities located in the Participating State of Hawaii authorized by that State's statutes to utilize State contracts.
2. Participation: All jurisdictions located within the State of Hawaii, which have obtained prior written approval by its Chief Procurement Officer, will be allowed to purchase from the Master Agreement. Private nonprofit health or human services organizations with current purchase of service contracts governed by Hawaii Revised Statutes (HRS) chapter 103F are eligible to participate in the SPO price/vendor list contracts upon mutual agreement between the Contractor and the non-profit. (Each such participating jurisdiction and participating nonprofit is hereinafter referred to as a "Participating Entity"). Issues of interpretation and eligibility for participation are solely within the authority of the Administrator, State Procurement Office.
3. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name:	Katelyn Rispoli
Address:	300 Davidson Avenue, Somerset, NJ 08873
Telephone:	(732) 854-8425
Fax:	N/A
Email:	Katelyn_rispoli@shi.com

CLOUD AND SOFTWARE SOLUTIONS

Led by the State of **Utah**

Participating State

Name:	Matthew Chow
Address:	State Procurement Office 1151 Punchbowl Street, Room 416 Honolulu, HI 96813
Telephone:	(808) 586-0577
Fax:	(808) 586-0570
Email:	matthew.m.chow@hawaii.gov

4. Participating State Modifications or Additions to the Master Agreement: These modifications or additions apply only to actions and relationships within the Participating State and its Entities.

☒ The following changes are modifying or supplementing the Master Agreement terms and conditions.

Changes:

A. eProcurement System and Marketplace

The State of Hawaii, State Procurement Office, has instituted a statewide eProcurement system, Aloha eBuys. Periscope Holdings, Inc. ("Periscope"), the State's eProcurement system provider, has implemented Aloha eBuys, which will allow Participating Entities to easily search and purchase from this price/vendor list contract. Therefore, Contractor acknowledges and agrees to the following, which requirements are separate from and additive to any of Contractor's requirements under the NASPO ValuePoint Master Agreement.

- i. Remittance of the VCAF – On a quarterly basis, and at the same time as the submission of the Quarterly Sales Report per the above, the Contractor shall remit the VCAF via Automated Clearing House (ACH) transaction directly to Periscope using the Reconciler portal, or as otherwise reasonably directed by Periscope or the State, no later than thirty (30) days after the end of each calendar quarter. The calendar quarters will end September 30, December 31, March 31, and June 30 of each year. Periscope's or the State's receipt or acceptance of any Quarterly Sales Report and/or VCAF furnished pursuant to the Contract shall not preclude Periscope or the State from challenging the validity thereof at any time. Failure to remit the Quarterly Sales Report and/or VCAF timely and accurately may result in Contractor's goods and/or services being made ineligible for purchase through the Aloha eBuys marketplace. Continued non-compliance by the Contractor may result in the Contractor

CLOUD AND SOFTWARE SOLUTIONS
Led by the State of **Utah**

being found in default of the Contract and, thus, may be subject to termination. Assistance with VCAF remittance is available from the Periscope Customer Service by email or telephone, which contact information shall be providing during Contractor's onboarding.

- ii. Catalog Implementation – Contractor shall cooperate with State and/or Periscope as requested, including attendance of meetings, to include and maintain throughout the term an Aloha eBuys marketplace catalog of products and services consistent with and limited to the Contract items. Contractor may choose one of the following catalog options.
 - a. Hosted Catalog – Contractor shall provide a list of its awarded products and services (including product name, descriptions, images, relevant specifications, keyword search terms, etc.) and pricing consistent with the Contract and in the electronic format provided by Periscope. The product and service list may only provide the awarded products and services at prices listed in the Contract, including quantity and other discounts. In order to maintain the most up-to-date version of the product and service list in compliance with Contract terms, Contractor must provide updated product and service pricing information via electronic format approved by Periscope at least annually but no more than four times per year or as otherwise permitted by the Contract.
 - b. Punchout Catalog – Contractor shall “punch out” to its own online catalog, provided that its own online catalog is capable of being integrated with the Aloha eBuys marketplace via Commerce eXtensible Markup Language. Contractor's punchout catalog may only provide the awarded products and services at prices listed in the Contract, including quantity and other discounts. Contractor must validate its punchout catalog is current by providing a written update to Periscope every four (4) months (or as otherwise provided in the Contract), verifying that Contractor has audited the offered products and services and pricing.
 - c. Marketplace Presence – If the Contractor does not have a product listing to create a hosted or punchout catalog, they shall establish a marketplace presence that includes detailed Contractor information contact details, marketing materials, website URLs showcasing their awarded products and services, and any additional resources to assist buyers in making purchases. Any pricing displayed must be consistent with the prices listed in the contract, ensuring transparency and alignment for potential buyers.

CLOUD AND SOFTWARE SOLUTIONS
Led by the State of **Utah**

Any price stated by Contractor under the Contract (including in its hosted or punchout catalog) shall be inclusive of the VCAF, and Contractor shall not reflect the VCAF as a separate line item on customer quotes and invoices.

Contractor shall 1) attend a vendor onboarding meeting with Periscope within thirty (30) days of the date of execution of this Amendment, and 2) complete upload of the hosted catalog or integration of the punchout catalog as well as the approval process(es) within ninety (90) calendar days of the date of execution of this Amendment. Contractor shall cooperate with State and Periscope for any other reasonable requests to ensure a catalog's accurate depiction of the Contract.

Any changes to Contractor's catalog permitted by the Contract must be pre-approved in writing by the State.

- iii. Vendor and Contract Performance Reviews – The State and/or Periscope may reasonably request Contractor to participate virtually in an annual business review, for which review Contractor shall provide Contract sales information as well as marketing action plans, target strategies and staff training plans and requirements designed to grow utilization of the Contract. Periscope shall also provide and discuss Quarterly Sales Reporting and VCAF remittance compliance data.
- iv. Retention and Inspection of Records and Audit – The Contractor shall keep records of all Sales in sufficient detail to enable the State or Periscope to determine the VCAF payable by the Contractor. The State and/or Periscope may examine and audit, at its own expense, Contractor's Sales records and Sales Reports for completeness and accuracy. If such examination reveals underpayment of the VCAF, the Contractor shall immediately pay to Periscope the amount of deficiency. If the examination reveals an underpayment of 5% or more, then the Contractor shall reimburse the State and Periscope for the cost of the audit.

B. Quarterly Sales Reporting

The Contractor shall be required to submit a quarterly report documenting all Sales made under the Contract ("Quarterly Sales Report"). "Sales" shall mean total invoices for gross purchases, less any credits, taxes, regulatory fees, and separately stated shipping charges not included in unit prices, procured on or utilizing pricing and/or other terms of this Contract, regardless of the purchase process. The Quarterly Sales Report shall be submitted directly to Periscope using the Reconciler portal (Periscope's reporting tool to which a link shall be provided to Contractor), or otherwise as reasonably directed by Periscope or State. Quarterly Sales Report will include any periods less than a full calendar quarter if Amendment and/or Contract does not start at the first day of a quarter or end on the last day of the quarter.

CLOUD AND SOFTWARE SOLUTIONS

Led by the State of **Utah**

Contractor shall submit one Quarterly Sales Report for each contract for each reporting period in accordance with the following schedule:

	Date Range	Due No Later Than
Fiscal Year, Quarter 1	July 1 – September 30	October 31
Fiscal Year, Quarter 2	October 1 – December 31	January 31
Fiscal Year, Quarter 3	January 1 – March 31	April 30
Fiscal Year, Quarter 4	April 1 – June 30	July 31

The Quarterly Sales Report must contain the following information:

- i. Complete and accurate details of all Sales, credits, returns, refunds, and the like for the reporting quarter;
- ii. Purchasing Participating Entity and type;
- iii. Product/service description, unit price, quantity and total sale amount;
- iv. Invoice number and date;
- v. Total Vendor Collected Administrative Fee amount due for the reporting quarter. "Vendor Collected Administrative Fee (VCAF)" shall mean that for all Sales made under or utilizing the pricing or other terms of the Contract that have been invoiced, the Contractor shall remit a VCAF in the amount of one and one-half percent (1.5%) of all Sales to Periscope on behalf of the State;
- vi. Such other information as the State and Periscope may reasonably request; and
- vii. If no Sales were made during the reporting quarter, then a Quarterly Sales Report shall still be submitted showing zero Sales and zero VCAF due.

Initiation and submission of the Quarterly Sales Report are the responsibility of the Contractor without prompting or notification by Periscope or the State, and Periscope and the State assume no responsibility for any Contractor's failure to meet its sales reporting and fee remittance obligations. The State reserves the right to contact Contractor at any time to request that Contractor attest to the amounts reported to have been paid to them by Participating Entities.

The State and Periscope shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided.

C. Validity of this Addendum

Any of its terms or provisions, as well as the rights and duties of the parties in this Addendum, shall be governed by the laws of the State of Hawaii. The attached Exhibit A, Attorney General's General Conditions, is made part of this Addendum. Any action at law or in equity to enforce or interpret the provisions of this Addendum shall be brought in a court of competent jurisdiction in Honolulu, Hawaii.

CLOUD AND SOFTWARE SOLUTIONS
Led by the State of **Utah**

D. Inspection of Facilities

Pursuant to HRS § 103D-316, the Participating State, at reasonable times, may inspect the part of the plant or place of business of the Contractor or any subcontractor that is related to the performance of a Master Agreement and this Addendum.

E. Campaign Contributions

The Contractor is notified of the applicability of HRS § 11-355, which prohibits campaign contributions from Contractor during the term of the Addendum if the contractor is paid with funds appropriated by the Hawaii State Legislature.

F. Non-Mandatory

Purchases by State of Hawaii government entities under this Master Agreement are not mandatory. This addendum is non-exclusive and any conflict among documents shall follow the Order of Precedence described in the Master Agreement. If there is no Order of Precedence in the Master Agreement, it shall be as follows:

- i. Hawaii Participating Addendum ("PA").
- ii. Master Agreement, including all attachments thereto;
- iii. A Purchase Order, Service Level Agreement, and/or Lease Agreement issued against the Master Agreement;
- iv. The solicitation or, if separately executed after award, the Lead State's bilateral agreement that integrates applicable provisions;
- v. Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State.

G. pCard

The State of Hawaii's purchasing card (pCard) is required to be used by the State's executive departments/agencies (excluding the Department of Education, School Facilities Authority, the Hawaii Health System Corporation, the Office of Hawaiian Affairs, and the University of Hawaii) for all orders totaling less than \$2,500. For purchases of \$2,500 or more, agencies may use the pCard, subject to its credit limit or issue a purchase order.

H. Compliance

Pursuant to HRS §103D-310(c), if Contractor is doing business in the Participating State, Contractor is required to comply with all laws governing entities doing business in the Participating State, including the following HRS chapters.

- i. Chapter 237, General Excise Tax Law;

CLOUD AND SOFTWARE SOLUTIONS
Led by the State of Utah

- ii. Chapter 383, Hawaii Employment Security Law;
- iii. Chapter 386, Workers' Compensation;
- iv. Chapter 392, Temporary Disability Insurance;
- v. Chapter 393, Prepaid Health Care Act; and

A Certificate of Good Standing is required for entities doing business in the State.

The Hawaii Compliance Express (HCE) is utilized for verification of compliance. The SPO will conduct periodic checks to confirm Contractor's compliance via HCE throughout the term of the Addendum.

Alternatively, Contractors not utilizing HCE to demonstrate compliance shall provide paper certificates to the SPO as instructed below. All certificates must be valid on the date they are received by the SPO. All applications for applicable clearances are the responsibility of the Contractor.

HRS Chapter 237 tax clearance requirement. Pursuant to Section 103D-328, HRS, Contractor shall be required to submit a tax clearance certificate issued by the Hawaii State Department of Taxation (DOTAX) and the Internal Revenue Service (IRS). Tax clearance certificates issued after September 3, 2019, will have a scannable QR code that can be validated. This enables tax clearance certificates to be processed electronically and printed by the taxpayer. The QR code can be scanned using a web enabled device, such as a smart phone, to confirm authenticity and validity. A tax clearance certificate may be revoked by the Department when the taxpayer falls out of tax compliance.

The Tax Clearance Application, Form A-6, and its completion and filing instructions, are available on the DOTAX website: <http://tax.hawaii.gov/forms/>.

HRS Chapters 383 (Unemployment Insurance), 386 (Workers' Compensation), 392 (Temporary Disability Insurance), and 393 (Prepaid Health Care) requirements. Pursuant to Section 103D-310(c) Contractor shall be required to submit a certificate of compliance issued by the Hawaii State Department of Labor and Industrial Relations (DLIR). The certificate is valid for six (6) months from the date of issue. A photocopy of the certificate is acceptable to the SPO.

The DLIR Form LIR#27 Application for Certificate of Compliance with Section 3-122-112, HAR, and its filing instructions are available on the DLIR website: <http://labor.hawaii.gov/forms/>.

Compliance with Section 103D-310(c), HRS, for an entity doing business in the State. Contractor shall be required to submit a Certificate of Good Standing (COGS) issued by the State of Hawaii Department of Commerce and Consumer Affairs (DCCA) – Business Registration Division (BREG). The Certificate is valid for six (6) months from date of issue. A photocopy of the certificate is acceptable to the SPO.

CLOUD AND SOFTWARE SOLUTIONS

Led by the State of Utah

To obtain the Certificate, the Contractor must be registered with the BREG. A sole proprietorship is not required to register with the BREG and is therefore not required to submit the certificate.

For more information regarding online business registration and the COGS is available at <http://cca.hawaii.gov/breg/>.

I. Effective Date and Contract Period

This Addendum is effective upon the date of execution by the Participating State and shall continue for the term set forth in the Master Agreement.

J. Licensing

Contractors must be properly licensed and capable of performing the Work as described in the Master Agreement, in accordance with the Professional and Vocational licensing laws of the state. Contractors under Participating Addendums must maintain all required licenses through the duration of the contract and Participating Addendum.

K. Insurance

The Contractor shall maintain in full force and effect during the life of this contract, liability and property damage insurance to protect the Contractor and its Subcontractors, if any, from claims for damages for personal injury, accidental death and property damage which may arise from operations under this contract, whether such operations be by the Contractor or by Subcontractor or anyone directly or indirectly employed by either of them. If any Subcontractor is involved, the insurance policy or policies shall name the Subcontractor as additional insured.

As an alternative to the Contractor providing insurance to cover operations performed by a Subcontractor and naming the Subcontractor as additional insured, the Contractor may require the Subcontractor to provide its own insurance, which meets the requirements herein. It is understood that a Subcontractor's insurance policy or policies are in addition to the Contractor's own policy or policies.

The following minimum insurance coverage(s) and limit(s) shall be provided by the Contractor, including its Subcontractor(s) where appropriate.

Coverage

Limits

Commercial General Liability
(occurrence form)

\$1,000,000 per occurrence
\$2,000,000 aggregate

CLOUD AND SOFTWARE SOLUTIONS
Led by the State of **Utah**

Automobile Liability

\$1,000,000 per accident

Cyber Liability covering claims and losses with respect to network, internet (Cloud) or other data disclosure risks (such as data breaches, releases of Confidential Information, unauthorized access/use of information, and identity theft) within limits of not less than \$1,000,000 per claim and \$2,000,000 aggregate.

Each insurance policy required by this contract, including a Subcontractor's policy, shall contain the following clauses:

- i. "The State of Hawaii is added as an additional insured as respects to operations performed for the State of Hawaii."
- ii. "It is agreed that any insurance maintained by the State of Hawaii will apply in excess of, and not contribute with, insurance provided by this policy."

A Waiver of Subrogation shall apply to the General Liability, Automobile Liability and Worker's Compensation insurance policies and shall be in favor of the State of Hawaii.

The Contractor agrees to deposit with the State of Hawaii certificate(s) of insurance necessary to satisfy the State that the insurance provisions of this Addendum have been complied with and to keep such insurance in effect and the certificate(s) therefore on deposit with the State during the entire term of the price/vendor list and price/vendor list extensions, if any, including those of its Subcontractor(s), where appropriate. Upon request, Contractor shall provide a copy of the policy or policies or shall allow the State to inspect a copy of the policy or policies.

Failure of the Contractor to provide and keep in force such insurance shall be regarded as material default, entitling the State to exercise any or all the remedies provided in the contract and this RFP for a default by the Contractor.

The procuring of such required insurance shall not be construed to limit the Contractor's liability hereunder nor to fulfill the indemnification provisions and requirements of this RFP. Notwithstanding said policy or policies of insurance, the Contractor shall be obliged for the full and total amount of any damage, injury, or loss caused by negligence or neglect connected with this price/vendor list.

L. Special Provisions for Purchases During Declared Disasters

The attached Exhibit B, Required FEMA Disaster Provisions are made part of this addendum. FEMA requires inclusion of certain provisions for the State to receive reimbursement.

M. Hawaii Information Technology Disability Access Standards

The attached Exhibit C, Hawaii Electronic Information Technology Disability Standards is made a part of this Addendum. All electronic information technology developed or provided under this contract or procurement shall comply with the applicable requirements of the Hawaii Electronic Information Technology Disability Access Standards (Access Standards).

N. If applicable, the Purchasing Agency shall specify in the applicable Purchase Order, Service Level Agreement, or Statement of Work/specifications the required GovRAMP status (e.g., Authorized, Provisionally Authorized, Ready, Core, or Progressing Snapshot Program) and any required overlays or supplemental compliance documentation for the Products and Services being procured.

- **GovRAMP Requirements.** The scope of this Participating Addendum is limited to only Products and Services meeting one of the following selected GovRAMP statuses:

☐ **Authorized Status:** Authorized, also referred to as full authorization, is the highest verification level which shows that a product has a proven and complete security package that has been reviewed by a Third-Party Assessing Organization ("3PAO") to ensure compliance with the NIST 800-53 required controls by impact level. The GovRAMP Project Management Office ("PMO") provides independent validation and verification of the security package which is then reviewed by the Sponsoring body before full approval is granted. These products participate in monthly continuous monitoring. Contractor must provide proof of current GovRAMP Authorized Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter. Participating Entity or a Purchasing Entity may also require supplementation of this status with an overlay (e.g., CJIS overlay). If an overlay is required herein or in an Order, Contractor must provide proof of its compliance with the applicable requirements in the form of a GovRAMP Letter.

☐ **Provisionally Authorized Status:** A product meets the Authorization requirements, but one or more of the following is true: one of the product's interconnected technologies is not GovRAMP or FedRAMP Authorized and/or during the PMO review, it is identified that one or more deficiencies exists that the PMO and Sponsoring Body agree could reasonably be remediated through the issuance of a Plan of Action and Milestone entry and that those deficiencies do not materially affect the overall security posture of the product. These products also participate in monthly continuous monitoring. Contractor must provide proof of current GovRAMP Provisionally Authorized Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter.

CLOUD AND SOFTWARE SOLUTIONS

Led by the State of Utah

- ☐ **Ready Status:** A Ready status indicates that the product meets GovRAMP's Minimum Mandatory Requirements and most critical controls, with an annual readiness assessment completed by a 3PAO, along with monthly continuous monitoring requirements. Contractor must provide proof of current GovRAMP Ready Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter.
 - ☐ **Core Status:** The GovRAMP Core security status provides an early step in verified GovRAMP statuses to demonstrate the maturity of a cloud product's security program. This early step demonstrates achievement of baseline NIST 800-53 Rev. 5 controls and documentation requirements as assessed and validated by the GovRAMP PMO, along with quarterly continuous monitoring. Contractor must provide proof of current GovRAMP Core Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter.
 - ☐ **Progressing Snapshot Program:** The GovRAMP Progressing Security Snapshot Program is an ongoing security maturity assessment for cloud products based on the 40 most impactful NIST 800-53 Rev. 5 controls as determined by the MITRE ATT&CK® Framework. The Progressing Security Snapshot Program helps service providers begin their cybersecurity journey while offering governments an initial level of insight into the risk maturity of suppliers' cloud products on an ongoing basis. Snapshots are completed on a quarterly basis to show governments and Providers where the product is on its cyber maturity journey. Contractor must provide proof of enrollment in the form of a GovRAMP letter and the most recent Snapshot score letter for the applicable Product(s) and Service(s) and must submit ongoing verification of progress until a verified status is achieved.
- **Application of GovRAMP Requirements.** Regardless of the status(es) selected, Contractor must provision access to Continuous Monitoring or Quarterly Progress Reports to the Participating Entity or Purchasing Agency, as applicable, for the duration of the Participating Addendum or Order, respectively.

5. **Lease Agreements:** Leasing is not authorized by this Addendum.

6. **Subcontractors:** All contractors, dealers, and resellers authorized in the State of Hawaii, as shown on the dedicated Contractor (cooperative contract) website, are approved to provide sales and service support to participants in the NASPO ValuePoint Master Agreement. The contractor's dealer participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement. Subcontractors are allowed under this Addendum.

CLOUD AND SOFTWARE SOLUTIONS
Led by the State of **Utah**

7. Orders: Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.
8. Freight Charges (unless otherwise stated in the master contract): Prices proposed will be the delivered price to any state agency or political subdivision. All deliveries will be F.O.B. destination with all transportation and handling charges paid by the Contractor. Responsibility and liability for loss or damage will remain with Contractor until final inspection and acceptance when responsibility will pass to the Buyer except as to latent defects, fraud, and Contractor's warranty obligations. Any portion of a full order originally shipped without transportation charges (that failed to ship with the original order, thereby becoming back-ordered) will also be shipped without transportation charges.
9. Purchase Order and Payment Instructions: All purchase orders issued by Participating Entities under this Addendum shall include the Participating State contract number: SPO Vendor List Contract No. 26-13 and the NASPO ValuePoint Master Agreement Number LS5021.

Purchase Orders and Payments shall be made to SHI International Corp.

10. Invoices and Payment Instructions: Contractor(s) shall forward original invoice(s), directly to the ordering agency. The GET or use tax and county surcharge may be added to the invoice as a separate line item and shall not exceed the current max pass-on tax rate(s) for each island.

County surcharges on state general excise (GE) tax or Use tax may be visibly passed on but is not required. For more information on county surcharges and the max pass-on tax rate, please visit the Department of Taxation's website at <http://tax.hawaii.gov/geninfo/countysurcharge>.

Pursuant to HRS § 103-10, Participating State and any agency of the Participating State or any county, shall have thirty (30) calendar days after receipt of invoice or satisfactory delivery of goods to make payment. Any interest for delinquent payment shall be as allowed by HRS § 103-10.

11. Participating Entity as Individual Customer: Each Participating Entity shall be treated as an individual customer. Except to the extent modified by this Addendum, each Participating Entity will be responsible to follow the terms and conditions of the Master Agreement; and will have the same rights and responsibilities for their purchases as the

Lead State has in the Master Agreement. Each Participating Entity will be responsible for its own charges, fees, and liabilities. Each Participating Entity will have the same rights to any indemnity or to recover any costs allowed in the Master Agreement for their purchases. The Contractor will apply the charges to each Participating Entity individually.

12. Entire Contract: This Addendum, the Master Agreement, and the Attorney General's General Conditions, set forth the entire agreement, and all the conditions, understandings, promises, warranties, and representations among the parties with respect to this Addendum and the Master Agreement, and supersedes any prior communications, representations, or agreements whether, oral or written, with respect to the subject matter hereof.

Terms and conditions inconsistent with, contrary or in addition to the terms and conditions of this Addendum, the Master Agreement, and the Attorney General's General Conditions that are included in any purchase order or other document shall be void. The terms and conditions of this Addendum, the Master Agreement, and the Attorney General's General Conditions, shall govern in the case of any such inconsistent, contrary, or additional terms.

CLOUD AND SOFTWARE SOLUTIONS

Led by the State of Utah

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

Participating State: STATE OF HAWAII	Contractor: SHI INTERNATIONAL CORP
Signature: 	Signature: 
Name: BONNIE KAHAKUI	Name: PAUL LINHARDT
Title: Administrator, SPO	Title: Sr. Lead Contracts Specialist
Date: 07/30/2026	Date: 07/28/2026

APPROVED AS TO FORM:



07/29/2026

Deputy Attorney General

For questions on executing a participating addendum, please contact:

NASPO ValuePoint

Cooperative Development Coordinator:	Nick Hughes
Telephone:	
Email:	nhughes@naspo.org

[Please email fully executed PDF copy of this document to

PA@naspovaluepoint.org

to support documentation of participation and posting in appropriate data bases.]

GENERAL CONDITIONS

Table of Contents

Page(s)

1.	Coordination of Services by the STATE.....	2
2.	Relationship of Parties: Independent Contractor Status and Responsibilities, Including Tax Responsibilities.....	2
3.	Personnel Requirements	3
4.	Nondiscrimination	3
5.	Conflicts of Interest	3
6.	Subcontracts and Assignments	3
7.	Indemnification and Defense.....	4
8.	Cost of Litigation.....	4
9.	Liquidated Damages	4
10.	STATE'S Right of Offset.....	4
11.	Disputes	4
12.	Suspension of Contract.....	4
13.	Termination for Default.....	5
14.	Termination for Convenience	6
15.	Claims Based on the Agency Procurement Officer's Actions or Omissions.....	8
16.	Costs and Expenses	8
17.	Payment Procedures; Final Payment; Tax Clearance	9
18.	Federal Funds	9
19.	Modifications of Contract.....	9
20.	Change Order.....	10
21.	Price Adjustment	11
22.	Variation in Quantity for Definite Quantity Contracts	11
23.	Changes in Cost-Reimbursement Contract.....	11
24.	Confidentiality of Material	12
25.	Publicity.....	12
26.	Ownership Rights and Copyright	12
27.	Liens and Warranties	12
28.	Audit of Books and Records of the CONTRACTOR.....	13
29.	Cost or Pricing Data	13
30.	Audit of Cost or Pricing Data	13
31.	Records Retention.....	13
32.	Antitrust Claims.....	13
33.	Patented Articles.....	13
34.	Governing Law	14
35.	Compliance with Laws	14
36.	Conflict between General Conditions and Procurement Rules	14
37.	Entire Contract.....	14
38.	Severability	14
39.	Waiver	14
40.	Pollution Control	14
41.	Campaign Contributions.....	14
42.	Confidentiality of Personal Information.....	14

GENERAL CONDITIONS

1. Coordination of Services by the STATE. The head of the purchasing agency ("HOPA") (which term includes the designee of the HOPA) shall coordinate the services to be provided by the CONTRACTOR in order to complete the performance required in the Contract. The CONTRACTOR shall maintain communications with HOPA at all stages of the CONTRACTOR'S work, and submit to HOPA for resolution any questions which may arise as to the performance of this Contract. "Purchasing agency" as used in these General Conditions means and includes any governmental body which is authorized under chapter 103D, HRS, or its implementing rules and procedures, or by way of delegation, to enter into contracts for the procurement of goods or services or both.
2. Relationship of Parties: Independent Contractor Status and Responsibilities, Including Tax Responsibilities.
 - a. In the performance of services required under this Contract, the CONTRACTOR is an "independent contractor," with the authority and responsibility to control and direct the performance and details of the work and services required under this Contract; however, the STATE shall have a general right to inspect work in progress to determine whether, in the STATE'S opinion, the services are being performed by the CONTRACTOR in compliance with this Contract. Unless otherwise provided by special condition, it is understood that the STATE does not agree to use the CONTRACTOR exclusively, and that the CONTRACTOR is free to contract to provide services to other individuals or entities while under contract with the STATE.
 - b. The CONTRACTOR and the CONTRACTOR'S employees and agents are not by reason of this Contract, agents or employees of the State for any purpose, and the CONTRACTOR and the CONTRACTOR'S employees and agents shall not be entitled to claim or receive from the State any vacation, sick leave, retirement, workers' compensation, unemployment insurance, or other benefits provided to state employees.
 - c. The CONTRACTOR shall be responsible for the accuracy, completeness, and adequacy of the CONTRACTOR'S performance under this Contract. Furthermore, the CONTRACTOR intentionally, voluntarily, and knowingly assumes the sole and entire liability to the CONTRACTOR'S employees and agents, and to any individual not a party to this Contract, for all loss, damage, or injury caused by the CONTRACTOR, or the CONTRACTOR'S employees or agents in the course of their employment.
 - d. The CONTRACTOR shall be responsible for payment of all applicable federal, state, and county taxes and fees which may become due and owing by the CONTRACTOR by reason of this Contract, including but not limited to (i) income taxes, (ii) employment related fees, assessments, and taxes, and (iii) general excise taxes. The CONTRACTOR also is responsible for obtaining all licenses, permits, and certificates that may be required in order to perform this Contract.
 - e. The CONTRACTOR shall obtain a general excise tax license from the Department of Taxation, State of Hawaii, in accordance with section 237-9, HRS, and shall comply with all requirements thereof. The CONTRACTOR shall obtain a tax clearance certificate from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of the Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR have been paid and submit the same to the STATE prior to commencing any performance under this Contract. The CONTRACTOR shall also be solely responsible for meeting all requirements necessary to obtain the tax clearance certificate required for final payment under sections 103-53 and 103D-328, HRS, and paragraph 17 of these General Conditions.
 - f. The CONTRACTOR is responsible for securing all employee-related insurance coverage for the CONTRACTOR and the CONTRACTOR'S employees and agents that is or may be required by law, and for payment of all premiums, costs, and other liabilities associated with securing the insurance coverage.

- g. The CONTRACTOR shall obtain a certificate of compliance issued by the Department of Labor and Industrial Relations, State of Hawaii, in accordance with section 103D-310, HRS, and section 3-122-112, HAR, that is current within six months of the date of issuance.
- h. The CONTRACTOR shall obtain a certificate of good standing issued by the Department of Commerce and Consumer Affairs, State of Hawaii, in accordance with section 103D-310, HRS, and section 3-122-112, HAR, that is current within six months of the date of issuance.
- i. In lieu of the above certificates from the Department of Taxation, Labor and Industrial Relations, and Commerce and Consumer Affairs, the CONTRACTOR may submit proof of compliance through the State Procurement Office's designated certification process.

3. Personnel Requirements.

- a. The CONTRACTOR shall secure, at the CONTRACTOR'S own expense, all personnel required to perform this Contract.
- b. The CONTRACTOR shall ensure that the CONTRACTOR'S employees or agents are experienced and fully qualified to engage in the activities and perform the services required under this Contract, and that all applicable licensing and operating requirements imposed or required under federal, state, or county law, and all applicable accreditation and other standards of quality generally accepted in the field of the activities of such employees and agents are complied with and satisfied.

4. Nondiscrimination. No person performing work under this Contract, including any subcontractor, employee, or agent of the CONTRACTOR, shall engage in any discrimination that is prohibited by any applicable federal, state, or county law.

5. Conflicts of Interest. The CONTRACTOR represents that neither the CONTRACTOR, nor any employee or agent of the CONTRACTOR, presently has any interest, and promises that no such interest, direct or indirect, shall be acquired, that would or might conflict in any manner or degree with the CONTRACTOR'S performance under this Contract.

6. Subcontracts and Assignments. The CONTRACTOR shall not assign or subcontract any of the CONTRACTOR'S duties, obligations, or interests under this Contract and no such assignment or subcontract shall be effective unless (i) the CONTRACTOR obtains the prior written consent of the STATE, and (ii) the CONTRACTOR'S assignee or subcontractor submits to the STATE a tax clearance certificate from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR'S assignee or subcontractor have been paid. Additionally, no assignment by the CONTRACTOR of the CONTRACTOR'S right to compensation under this Contract shall be effective unless and until the assignment is approved by the Comptroller of the State of Hawaii, as provided in section 40-58, HRS.

- a. Recognition of a successor in interest. When in the best interest of the State, a successor in interest may be recognized in an assignment contract in which the STATE, the CONTRACTOR and the assignee or transferee (hereinafter referred to as the "Assignee") agree that:

- (1) The Assignee assumes all of the CONTRACTOR'S obligations;
- (2) The CONTRACTOR remains liable for all obligations under this Contract but waives all rights under this Contract as against the STATE; and
- (3) The CONTRACTOR shall continue to furnish, and the Assignee shall also furnish, all required bonds.

- b. Change of name. When the CONTRACTOR asks to change the name in which it holds this Contract with the STATE, the procurement officer of the purchasing agency (hereinafter referred to as the "Agency procurement officer") shall, upon receipt of a document acceptable or satisfactory to the

Agency procurement officer indicating such change of name (for example, an amendment to the CONTRACTOR'S articles of incorporation), enter into an amendment to this Contract with the CONTRACTOR to effect such a change of name. The amendment to this Contract changing the CONTRACTOR'S name shall specifically indicate that no other terms and conditions of this Contract are thereby changed.

- c. Reports. All assignment contracts and amendments to this Contract effecting changes of the CONTRACTOR'S name or novations hereunder shall be reported to the chief procurement officer (CPO) as defined in section 103D-203(a), HRS, within thirty days of the date that the assignment contract or amendment becomes effective.
 - d. Actions affecting more than one purchasing agency. Notwithstanding the provisions of subparagraphs 6a through 6c herein, when the CONTRACTOR holds contracts with more than one purchasing agency of the State, the assignment contracts and the novation and change of name amendments herein authorized shall be processed only through the CPO's office.
7. Indemnification and Defense. The CONTRACTOR shall defend, indemnify, and hold harmless the State of Hawaii, the contracting agency, and their officers, employees, and agents from and against all liability, loss, damage, cost, and expense, including all attorneys' fees, and all claims, suits, and demands therefore, arising out of or resulting from the acts or omissions of the CONTRACTOR or the CONTRACTOR'S employees, officers, agents, or subcontractors under this Contract. The provisions of this paragraph shall remain in full force and effect notwithstanding the expiration or early termination of this Contract.
 8. Cost of Litigation. In case the STATE shall, without any fault on its part, be made a party to any litigation commenced by or against the CONTRACTOR in connection with this Contract, the CONTRACTOR shall pay all costs and expenses incurred by or imposed on the STATE, including attorneys' fees.
 9. Liquidated Damages. When the CONTRACTOR is given notice of delay or nonperformance as specified in paragraph 13 (Termination for Default) and fails to cure in the time specified, it is agreed the CONTRACTOR shall pay to the STATE the amount, if any, set forth in this Contract per calendar day from the date set for cure until either (i) the STATE reasonably obtains similar goods or services, or both, if the CONTRACTOR is terminated for default, or (ii) until the CONTRACTOR provides the goods or services, or both, if the CONTRACTOR is not terminated for default. To the extent that the CONTRACTOR'S delay or nonperformance is excused under paragraph 13d (Excuse for Nonperformance or Delay Performance), liquidated damages shall not be assessable against the CONTRACTOR. The CONTRACTOR remains liable for damages caused other than by delay.
 10. STATE'S Right of Offset. The STATE may offset against any monies or other obligations the STATE owes to the CONTRACTOR under this Contract, any amounts owed to the State of Hawaii by the CONTRACTOR under this Contract or any other contracts, or pursuant to any law or other obligation owed to the State of Hawaii by the CONTRACTOR, including, without limitation, the payment of any taxes or levies of any kind or nature. The STATE will notify the CONTRACTOR in writing of any offset and the nature of such offset. For purposes of this paragraph, amounts owed to the State of Hawaii shall not include debts or obligations which have been liquidated, agreed to by the CONTRACTOR, and are covered by an installment payment or other settlement plan approved by the State of Hawaii, provided, however, that the CONTRACTOR shall be entitled to such exclusion only to the extent that the CONTRACTOR is current with, and not delinquent on, any payments or obligations owed to the State of Hawaii under such payment or other settlement plan.
 11. Disputes. Disputes shall be resolved in accordance with section 103D-703, HRS, and chapter 3-126, Hawaii Administrative Rules ("HAR"), as the same may be amended from time to time.
 12. Suspension of Contract. The STATE reserves the right at any time and for any reason to suspend this Contract for any reasonable period, upon written notice to the CONTRACTOR in accordance with the provisions herein.
 - a. Order to stop performance. The Agency procurement officer may, by written order to the CONTRACTOR, at any time, and without notice to any surety, require the CONTRACTOR to stop all or any part of the performance called for by this Contract. This order shall be for a specified

period not exceeding sixty (60) days after the order is delivered to the CONTRACTOR, unless the parties agree to any further period. Any such order shall be identified specifically as a stop performance order issued pursuant to this section. Stop performance orders shall include, as appropriate: (1) A clear description of the work to be suspended; (2) Instructions as to the issuance of further orders by the CONTRACTOR for material or services; (3) Guidance as to action to be taken on subcontracts; and (4) Other instructions and suggestions to the CONTRACTOR for minimizing costs. Upon receipt of such an order, the CONTRACTOR shall forthwith comply with its terms and suspend all performance under this Contract at the time stated, provided, however, the CONTRACTOR shall take all reasonable steps to minimize the occurrence of costs allocable to the performance covered by the order during the period of performance stoppage. Before the stop performance order expires, or within any further period to which the parties shall have agreed, the Agency procurement officer shall either:

- (1) Cancel the stop performance order; or
 - (2) Terminate the performance covered by such order as provided in the termination for default provision or the termination for convenience provision of this Contract.
- b. Cancellation or expiration of the order. If a stop performance order issued under this section is cancelled at any time during the period specified in the order, or if the period of the order or any extension thereof expires, the CONTRACTOR shall have the right to resume performance. An appropriate adjustment shall be made in the delivery schedule or contract price, or both, and the Contract shall be modified in writing accordingly, if:
- (1) The stop performance order results in an increase in the time required for, or in the CONTRACTOR'S cost properly allocable to, the performance of any part of this Contract; and
 - (2) The CONTRACTOR asserts a claim for such an adjustment within thirty (30) days after the end of the period of performance stoppage; provided that, if the Agency procurement officer decides that the facts justify such action, any such claim asserted may be received and acted upon at any time prior to final payment under this Contract.
- c. Termination of stopped performance. If a stop performance order is not cancelled and the performance covered by such order is terminated for default or convenience, the reasonable costs resulting from the stop performance order shall be allowable by adjustment or otherwise.
- d. Adjustment of price. Any adjustment in contract price made pursuant to this paragraph shall be determined in accordance with the price adjustment provision of this Contract.

13. Termination for Default.

- a. Default. If the CONTRACTOR refuses or fails to perform any of the provisions of this Contract with such diligence as will ensure its completion within the time specified in this Contract, or any extension thereof, otherwise fails to timely satisfy the Contract provisions, or commits any other substantial breach of this Contract, the Agency procurement officer may notify the CONTRACTOR in writing of the delay or non-performance and if not cured in ten (10) days or any longer time specified in writing by the Agency procurement officer, such officer may terminate the CONTRACTOR'S right to proceed with the Contract or such part of the Contract as to which there has been delay or a failure to properly perform. In the event of termination in whole or in part, the Agency procurement officer may procure similar goods or services in a manner and upon the terms deemed appropriate by the Agency procurement officer. The CONTRACTOR shall continue performance of the Contract to the extent it is not terminated and shall be liable for excess costs incurred in procuring similar goods or services.
- b. CONTRACTOR'S duties. Notwithstanding termination of the Contract and subject to any directions from the Agency procurement officer, the CONTRACTOR shall take timely, reasonable, and

necessary action to protect and preserve property in the possession of the CONTRACTOR in which the STATE has an interest.

- c. Compensation. Payment for completed goods and services delivered and accepted by the STATE shall be at the price set forth in the Contract. Payment for the protection and preservation of property shall be in an amount agreed upon by the CONTRACTOR and the Agency procurement officer. If the parties fail to agree, the Agency procurement officer shall set an amount subject to the CONTRACTOR'S rights under chapter 3-126, HAR. The STATE may withhold from amounts due the CONTRACTOR such sums as the Agency procurement officer deems to be necessary to protect the STATE against loss because of outstanding liens or claims and to reimburse the STATE for the excess costs expected to be incurred by the STATE in procuring similar goods and services.
- d. Excuse for nonperformance or delayed performance. The CONTRACTOR shall not be in default by reason of any failure in performance of this Contract in accordance with its terms, including any failure by the CONTRACTOR to make progress in the prosecution of the performance hereunder which endangers such performance, if the CONTRACTOR has notified the Agency procurement officer within fifteen (15) days after the cause of the delay and the failure arises out of causes such as: acts of God; acts of a public enemy; acts of the State and any other governmental body in its sovereign or contractual capacity; fires; floods; epidemics; quarantine restrictions; strikes or other labor disputes; freight embargoes; or unusually severe weather. If the failure to perform is caused by the failure of a subcontractor to perform or to make progress, and if such failure arises out of causes similar to those set forth above, the CONTRACTOR shall not be deemed to be in default, unless the goods and services to be furnished by the subcontractor were reasonably obtainable from other sources in sufficient time to permit the CONTRACTOR to meet the requirements of the Contract. Upon request of the CONTRACTOR, the Agency procurement officer shall ascertain the facts and extent of such failure, and, if such officer determines that any failure to perform was occasioned by any one or more of the excusable causes, and that, but for the excusable cause, the CONTRACTOR'S progress and performance would have met the terms of the Contract, the delivery schedule shall be revised accordingly, subject to the rights of the STATE under this Contract. As used in this paragraph, the term "subcontractor" means subcontractor at any tier.
- e. Erroneous termination for default. If, after notice of termination of the CONTRACTOR'S right to proceed under this paragraph, it is determined for any reason that the CONTRACTOR was not in default under this paragraph, or that the delay was excusable under the provisions of subparagraph 13d, "Excuse for nonperformance or delayed performance," the rights and obligations of the parties shall be the same as if the notice of termination had been issued pursuant to paragraph 14.
- f. Additional rights and remedies. The rights and remedies provided in this paragraph are in addition to any other rights and remedies provided by law or under this Contract.

14. Termination for Convenience.

- a. Termination. The Agency procurement officer may, when the interests of the STATE so require, terminate this Contract in whole or in part, for the convenience of the STATE. The Agency procurement officer shall give written notice of the termination to the CONTRACTOR specifying the part of the Contract terminated and when termination becomes effective.
- b. CONTRACTOR'S obligations. The CONTRACTOR shall incur no further obligations in connection with the terminated performance and on the date(s) set in the notice of termination the CONTRACTOR will stop performance to the extent specified. The CONTRACTOR shall also terminate outstanding orders and subcontracts as they relate to the terminated performance. The CONTRACTOR shall settle the liabilities and claims arising out of the termination of subcontracts and orders connected with the terminated performance subject to the STATE'S approval. The Agency procurement officer may direct the CONTRACTOR to assign the CONTRACTOR'S right, title, and interest under terminated orders or subcontracts to the STATE. The CONTRACTOR must still complete the performance not terminated by the notice of termination and may incur obligations as necessary to do so.

- c. Right to goods and work product. The Agency procurement officer may require the CONTRACTOR to transfer title and deliver to the STATE in the manner and to the extent directed by the Agency procurement officer:

- (1) Any completed goods or work product; and
- (2) The partially completed goods and materials, parts, tools, dies, jigs, fixtures, plans, drawings, information, and contract rights (hereinafter called "manufacturing material") as the CONTRACTOR has specifically produced or specially acquired for the performance of the terminated part of this Contract.

The CONTRACTOR shall, upon direction of the Agency procurement officer, protect and preserve property in the possession of the CONTRACTOR in which the STATE has an interest. If the Agency procurement officer does not exercise this right, the CONTRACTOR shall use best efforts to sell such goods and manufacturing materials. Use of this paragraph in no way implies that the STATE has breached the Contract by exercise of the termination for convenience provision.

- d. Compensation.

- (1) The CONTRACTOR shall submit a termination claim specifying the amounts due because of the termination for convenience together with the cost or pricing data, submitted to the extent required by chapter 3-122, HAR, bearing on such claim. If the CONTRACTOR fails to file a termination claim within one year from the effective date of termination, the Agency procurement officer may pay the CONTRACTOR, if at all, an amount set in accordance with subparagraph 14d(3) below.
- (2) The Agency procurement officer and the CONTRACTOR may agree to a settlement provided the CONTRACTOR has filed a termination claim supported by cost or pricing data submitted as required and that the settlement does not exceed the total Contract price plus settlement costs reduced by payments previously made by the STATE, the proceeds of any sales of goods and manufacturing materials under subparagraph 14c, and the Contract price of the performance not terminated.
- (3) Absent complete agreement under subparagraph 14d(2) the Agency procurement officer shall pay the CONTRACTOR the following amounts, provided payments agreed to under subparagraph 14d(2) shall not duplicate payments under this subparagraph for the following:
 - (A) Contract prices for goods or services accepted under the Contract;
 - (B) Costs incurred in preparing to perform and performing the terminated portion of the performance plus a fair and reasonable profit on such portion of the performance, such profit shall not include anticipatory profit or consequential damages, less amounts paid or to be paid for accepted goods or services; provided, however, that if it appears that the CONTRACTOR would have sustained a loss if the entire Contract would have been completed, no profit shall be allowed or included and the amount of compensation shall be reduced to reflect the anticipated rate of loss;
 - (C) Costs of settling and paying claims arising out of the termination of subcontracts or orders pursuant to subparagraph 14b. These costs must not include costs paid in accordance with subparagraph 14d(3)(B);
 - (D) The reasonable settlement costs of the CONTRACTOR, including accounting, legal, clerical, and other expenses reasonably necessary for the preparation of settlement claims and supporting data with respect to the terminated portion of the Contract and for the termination of subcontracts thereunder, together with reasonable storage, transportation, and other costs incurred in connection with the protection or disposition of property allocable to the terminated portion of this Contract. The total sum to be paid the CONTRACTOR under this subparagraph shall not exceed the

total Contract price plus the reasonable settlement costs of the CONTRACTOR reduced by the amount of payments otherwise made, the proceeds of any sales of supplies and manufacturing materials under subparagraph 14d(2), and the contract price of performance not terminated.

- (4) Costs claimed, agreed to, or established under subparagraphs 14d(2) and 14d(3) shall be in accordance with Chapter 3-123 (Cost Principles) of the Procurement Rules.

15. Claims Based on the Agency Procurement Officer's Actions or Omissions.

- a. Changes in scope. If any action or omission on the part of the Agency procurement officer (which term includes the designee of such officer for purposes of this paragraph 15) requiring performance changes within the scope of the Contract constitutes the basis for a claim by the CONTRACTOR for additional compensation, damages, or an extension of time for completion, the CONTRACTOR shall continue with performance of the Contract in compliance with the directions or orders of such officials, but by so doing, the CONTRACTOR shall not be deemed to have prejudiced any claim for additional compensation, damages, or an extension of time for completion; provided:
- (1) Written notice required. The CONTRACTOR shall give written notice to the Agency procurement officer:
 - (A) Prior to the commencement of the performance involved, if at that time the CONTRACTOR knows of the occurrence of such action or omission;
 - (B) Within thirty (30) days after the CONTRACTOR knows of the occurrence of such action or omission, if the CONTRACTOR did not have such knowledge prior to the commencement of the performance; or
 - (C) Within such further time as may be allowed by the Agency procurement officer in writing.
 - (2) Notice content. This notice shall state that the CONTRACTOR regards the act or omission as a reason which may entitle the CONTRACTOR to additional compensation, damages, or an extension of time. The Agency procurement officer, upon receipt of such notice, may rescind such action, remedy such omission, or take such other steps as may be deemed advisable in the discretion of the Agency procurement officer;
 - (3) Basis must be explained. The notice required by subparagraph 15a(1) describes as clearly as practicable at the time the reasons why the CONTRACTOR believes that additional compensation, damages, or an extension of time may be remedies to which the CONTRACTOR is entitled; and
 - (4) Claim must be justified. The CONTRACTOR must maintain and, upon request, make available to the Agency procurement officer within a reasonable time, detailed records to the extent practicable, and other documentation and evidence satisfactory to the STATE, justifying the claimed additional costs or an extension of time in connection with such changes.
- b. CONTRACTOR not excused. Nothing herein contained, however, shall excuse the CONTRACTOR from compliance with any rules or laws precluding any state officers and CONTRACTOR from acting in collusion or bad faith in issuing or performing change orders which are clearly not within the scope of the Contract.
- c. Price adjustment. Any adjustment in the price made pursuant to this paragraph shall be determined in accordance with the price adjustment provision of this Contract.

16. Costs and Expenses. Any reimbursement due the CONTRACTOR for per diem and transportation expenses under this Contract shall be subject to chapter 3-123 (Cost Principles), HAR, and the following guidelines:

- a. Reimbursement for air transportation shall be for actual cost or coach class air fare, whichever is less.
- b. Reimbursement for ground transportation costs shall not exceed the actual cost of renting an intermediate-sized vehicle.
- c. Unless prior written approval of the HOPA is obtained, reimbursement for subsistence allowance (i.e., hotel and meals, etc.) shall not exceed the applicable daily authorized rates for inter-island or out-of-state travel that are set forth in the current Governor's Executive Order authorizing adjustments in salaries and benefits for state officers and employees in the executive branch who are excluded from collective bargaining coverage.

17. Payment Procedures; Final Payment; Tax Clearance.

- a. Original invoices required. All payments under this Contract shall be made only upon submission by the CONTRACTOR of original invoices specifying the amount due and certifying that services requested under the Contract have been performed by the CONTRACTOR according to the Contract.
- b. Subject to available funds. Such payments are subject to availability of funds and allotment by the Director of Finance in accordance with chapter 37, HRS. Further, all payments shall be made in accordance with and subject to chapter 40, HRS.
- c. Prompt payment.
 - (1) Any money, other than retainage, paid to the CONTRACTOR shall be disbursed to subcontractors within ten (10) days after receipt of the money in accordance with the terms of the subcontract; provided that the subcontractor has met all the terms and conditions of the subcontract and there are no bona fide disputes; and
 - (2) Upon final payment to the CONTRACTOR, full payment to the subcontractor, including retainage, shall be made within ten (10) days after receipt of the money; provided that there are no bona fide disputes over the subcontractor's performance under the subcontract.
- d. Final payment. Final payment under this Contract shall be subject to sections 103-53 and 103D-328, HRS, which require a tax clearance from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR have been paid. Further, in accordance with section 3-122-112, HAR, CONTRACTOR shall provide a certificate affirming that the CONTRACTOR has remained in compliance with all applicable laws as required by this section.

18. Federal Funds. If this Contract is payable in whole or in part from federal funds, CONTRACTOR agrees that, as to the portion of the compensation under this Contract to be payable from federal funds, the CONTRACTOR shall be paid only from such funds received from the federal government, and shall not be paid from any other funds. Failure of the STATE to receive anticipated federal funds shall not be considered a breach by the STATE or an excuse for nonperformance by the CONTRACTOR.

19. Modifications of Contract.

- a. In writing. Any modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract permitted by this Contract shall be made by written amendment to this Contract, signed by the CONTRACTOR and the STATE, provided that change orders shall be made in accordance with paragraph 20 herein.
- b. No oral modification. No oral modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract shall be permitted.

- c. Agency procurement officer. By written order, at any time, and without notice to any surety, the Agency procurement officer may unilaterally order of the CONTRACTOR:
 - (A) Changes in the work within the scope of the Contract; and
 - (B) Changes in the time of performance of the Contract that do not alter the scope of the Contract work.
 - d. Adjustments of price or time for performance. If any modification increases or decreases the CONTRACTOR'S cost of, or the time required for, performance of any part of the work under this Contract, an adjustment shall be made and this Contract modified in writing accordingly. Any adjustment in contract price made pursuant to this clause shall be determined, where applicable, in accordance with the price adjustment clause of this Contract or as negotiated.
 - e. Claim barred after final payment. No claim by the CONTRACTOR for an adjustment hereunder shall be allowed if written modification of the Contract is not made prior to final payment under this Contract.
 - f. Claims not barred. In the absence of a written contract modification, nothing in this clause shall be deemed to restrict the CONTRACTOR'S right to pursue a claim under this Contract or for a breach of contract.
 - g. Head of the purchasing agency approval. If this is a professional services contract awarded pursuant to section 103D-303 or 103D-304, HRS, any modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract which increases the amount payable to the CONTRACTOR by at least \$25,000.00 and ten per cent (10%) or more of the initial contract price, must receive the prior approval of the head of the purchasing agency.
 - h. Tax clearance. The STATE may, at its discretion, require the CONTRACTOR to submit to the STATE, prior to the STATE'S approval of any modification, alteration, amendment, change, or extension of any term, provision, or condition of this Contract, a tax clearance from the Director of Taxation, State of Hawaii, and the Internal Revenue Service, U.S. Department of Treasury, showing that all delinquent taxes, if any, levied or accrued under state law and the Internal Revenue Code of 1986, as amended, against the CONTRACTOR have been paid.
 - i. Sole source contracts. Amendments to sole source contracts that would change the original scope of the Contract may only be made with the approval of the CPO. Annual renewal of a sole source contract for services should not be submitted as an amendment.
20. Change Order. The Agency procurement officer may, by a written order signed only by the STATE, at any time, and without notice to any surety, and subject to all appropriate adjustments, make changes within the general scope of this Contract in any one or more of the following:
- (1) Drawings, designs, or specifications, if the goods or services to be furnished are to be specially provided to the STATE in accordance therewith;
 - (2) Method of delivery; or
 - (3) Place of delivery.
- a. Adjustments of price or time for performance. If any change order increases or decreases the CONTRACTOR'S cost of, or the time required for, performance of any part of the work under this Contract, whether or not changed by the order, an adjustment shall be made and the Contract modified in writing accordingly. Any adjustment in the Contract price made pursuant to this provision shall be determined in accordance with the price adjustment provision of this Contract. Failure of the parties to agree to an adjustment shall not excuse the CONTRACTOR from proceeding with the Contract as changed, provided that the Agency procurement officer promptly and duly makes the provisional adjustments in payment or time for performance as may be reasonable. By

proceeding with the work, the CONTRACTOR shall not be deemed to have prejudiced any claim for additional compensation, or any extension of time for completion.

- b. Time period for claim. Within ten (10) days after receipt of a written change order under subparagraph 20a, unless the period is extended by the Agency procurement officer in writing, the CONTRACTOR shall respond with a claim for an adjustment. The requirement for a timely written response by CONTRACTOR cannot be waived and shall be a condition precedent to the assertion of a claim.
- c. Claim barred after final payment. No claim by the CONTRACTOR for an adjustment hereunder shall be allowed if a written response is not given prior to final payment under this Contract.
- d. Other claims not barred. In the absence of a change order, nothing in this paragraph 20 shall be deemed to restrict the CONTRACTOR'S right to pursue a claim under the Contract or for breach of contract.

21. Price Adjustment.

- a. Price adjustment. Any adjustment in the contract price pursuant to a provision in this Contract shall be made in one or more of the following ways:
 - (1) By agreement on a fixed price adjustment before commencement of the pertinent performance or as soon thereafter as practicable;
 - (2) By unit prices specified in the Contract or subsequently agreed upon;
 - (3) By the costs attributable to the event or situation covered by the provision, plus appropriate profit or fee, all as specified in the Contract or subsequently agreed upon;
 - (4) In such other manner as the parties may mutually agree; or
 - (5) In the absence of agreement between the parties, by a unilateral determination by the Agency procurement officer of the costs attributable to the event or situation covered by the provision, plus appropriate profit or fee, all as computed by the Agency procurement officer in accordance with generally accepted accounting principles and applicable sections of chapters 3-123 and 3-126, HAR.
- b. Submission of cost or pricing data. The CONTRACTOR shall provide cost or pricing data for any price adjustments subject to the provisions of chapter 3-122, HAR.

22. Variation in Quantity for Definite Quantity Contracts. Upon the agreement of the STATE and the CONTRACTOR, the quantity of goods or services, or both, if a definite quantity is specified in this Contract, may be increased by a maximum of ten per cent (10%); provided the unit prices will remain the same except for any price adjustments otherwise applicable; and the Agency procurement officer makes a written determination that such an increase will either be more economical than awarding another contract or that it would not be practical to award another contract.

23. Changes in Cost-Reimbursement Contract. If this Contract is a cost-reimbursement contract, the following provisions shall apply:

- a. The Agency procurement officer may at any time by written order, and without notice to the sureties, if any, make changes within the general scope of the Contract in any one or more of the following:
 - (1) Description of performance (Attachment 1);
 - (2) Time of performance (i.e., hours of the day, days of the week, etc.);
 - (3) Place of performance of services;

- (4) Drawings, designs, or specifications when the supplies to be furnished are to be specially manufactured for the STATE in accordance with the drawings, designs, or specifications;
 - (5) Method of shipment or packing of supplies; or
 - (6) Place of delivery.
- b. If any change causes an increase or decrease in the estimated cost of, or the time required for performance of, any part of the performance under this Contract, whether or not changed by the order, or otherwise affects any other terms and conditions of this Contract, the Agency procurement officer shall make an equitable adjustment in the (1) estimated cost, delivery or completion schedule, or both; (2) amount of any fixed fee; and (3) other affected terms and shall modify the Contract accordingly.
 - c. The CONTRACTOR must assert the CONTRACTOR'S rights to an adjustment under this provision within thirty (30) days from the day of receipt of the written order. However, if the Agency procurement officer decides that the facts justify it, the Agency procurement officer may receive and act upon a proposal submitted before final payment under the Contract.
 - d. Failure to agree to any adjustment shall be a dispute under paragraph 11 of this Contract. However, nothing in this provision shall excuse the CONTRACTOR from proceeding with the Contract as changed.
 - e. Notwithstanding the terms and conditions of subparagraphs 23a and 23b, the estimated cost of this Contract and, if this Contract is incrementally funded, the funds allotted for the performance of this Contract, shall not be increased or considered to be increased except by specific written modification of the Contract indicating the new contract estimated cost and, if this contract is incrementally funded, the new amount allotted to the contract.
24. Confidentiality of Material.
- a. All material given to or made available to the CONTRACTOR by virtue of this Contract, which is identified as proprietary or confidential information, will be safeguarded by the CONTRACTOR and shall not be disclosed to any individual or organization without the prior written approval of the STATE.
 - b. All information, data, or other material provided by the CONTRACTOR to the STATE shall be subject to the Uniform Information Practices Act, chapter 92F, HRS.
25. Publicity. The CONTRACTOR shall not refer to the STATE, or any office, agency, or officer thereof, or any state employee, including the HOPA, the CPO, the Agency procurement officer, or to the services or goods, or both, provided under this Contract, in any of the CONTRACTOR'S brochures, advertisements, or other publicity of the CONTRACTOR. All media contacts with the CONTRACTOR about the subject matter of this Contract shall be referred to the Agency procurement officer.
26. Ownership Rights and Copyright. The STATE shall have complete ownership of all material, both finished and unfinished, which is developed, prepared, assembled, or conceived by the CONTRACTOR pursuant to this Contract, and all such material shall be considered "works made for hire." All such material shall be delivered to the STATE upon expiration or termination of this Contract. The STATE, in its sole discretion, shall have the exclusive right to copyright any product, concept, or material developed, prepared, assembled, or conceived by the CONTRACTOR pursuant to this Contract.
27. Liens and Warranties. Goods provided under this Contract shall be provided free of all liens and provided together with all applicable warranties, or with the warranties described in the Contract documents, whichever are greater.

28. Audit of Books and Records of the CONTRACTOR. The STATE may, at reasonable times and places, audit the books and records of the CONTRACTOR, prospective contractor, subcontractor, or prospective subcontractor which are related to:
- a. The cost or pricing data, and
 - b. A state contract, including subcontracts, other than a firm fixed-price contract.
29. Cost or Pricing Data. Cost or pricing data must be submitted to the Agency procurement officer and timely certified as accurate for contracts over \$100,000 unless the contract is for a multiple-term or as otherwise specified by the Agency procurement officer. Unless otherwise required by the Agency procurement officer, cost or pricing data submission is not required for contracts awarded pursuant to competitive sealed bid procedures.
- If certified cost or pricing data are subsequently found to have been inaccurate, incomplete, or noncurrent as of the date stated in the certificate, the STATE is entitled to an adjustment of the contract price, including profit or fee, to exclude any significant sum by which the price, including profit or fee, was increased because of the defective data. It is presumed that overstated cost or pricing data increased the contract price in the amount of the defect plus related overhead and profit or fee. Therefore, unless there is a clear indication that the defective data was not used or relied upon, the price will be reduced in such amount.
30. Audit of Cost or Pricing Data. When cost or pricing principles are applicable, the STATE may require an audit of cost or pricing data.
31. Records Retention.
- (1) Upon any termination of this Contract or as otherwise required by applicable law, CONTRACTOR shall, pursuant to chapter 487R, HRS, destroy all copies (paper or electronic form) of personal information received from the STATE.
 - (2) The CONTRACTOR and any subcontractors shall maintain the files, books, and records that relate to the Contract, including any personal information created or received by the CONTRACTOR on behalf of the STATE, and any cost or pricing data, for at least three (3) years after the date of final payment under the Contract. The personal information shall continue to be confidential and shall only be disclosed as permitted or required by law. After the three (3) year, or longer retention period as required by law has ended, the files, books, and records that contain personal information shall be destroyed pursuant to chapter 487R, HRS or returned to the STATE at the request of the STATE.
32. Antitrust Claims. The STATE and the CONTRACTOR recognize that in actual economic practice, overcharges resulting from antitrust violations are in fact usually borne by the purchaser. Therefore, the CONTRACTOR hereby assigns to STATE any and all claims for overcharges as to goods and materials purchased in connection with this Contract, except as to overcharges which result from violations commencing after the price is established under this Contract and which are not passed on to the STATE under an escalation clause.
33. Patented Articles. The CONTRACTOR shall defend, indemnify, and hold harmless the STATE, and its officers, employees, and agents from and against all liability, loss, damage, cost, and expense, including all attorneys fees, and all claims, suits, and demands arising out of or resulting from any claims, demands, or actions by the patent holder for infringement or other improper or unauthorized use of any patented article, patented process, or patented appliance in connection with this Contract. The CONTRACTOR shall be solely responsible for correcting or curing to the satisfaction of the STATE any such infringement or improper or unauthorized use, including, without limitation: (a) furnishing at no cost to the STATE a substitute article, process, or appliance acceptable to the STATE, (b) paying royalties or other required payments to the patent holder, (c) obtaining proper authorizations or releases from the patent holder, and (d) furnishing such security to or making such arrangements with the patent holder as may be necessary to correct or cure any such infringement or improper or unauthorized use.

34. Governing Law. The validity of this Contract and any of its terms or provisions, as well as the rights and duties of the parties to this Contract, shall be governed by the laws of the State of Hawaii. Any action at law or in equity to enforce or interpret the provisions of this Contract shall be brought in a state court of competent jurisdiction in Honolulu, Hawaii.
35. Compliance with Laws. The CONTRACTOR shall comply with all federal, state, and county laws, ordinances, codes, rules, and regulations, as the same may be amended from time to time, that in any way affect the CONTRACTOR'S performance of this Contract.
36. Conflict Between General Conditions and Procurement Rules. In the event of a conflict between the General Conditions and the procurement rules, the procurement rules in effect on the date this Contract became effective shall control and are hereby incorporated by reference.
37. Entire Contract. This Contract sets forth all of the agreements, conditions, understandings, promises, warranties, and representations between the STATE and the CONTRACTOR relative to this Contract. This Contract supersedes all prior agreements, conditions, understandings, promises, warranties, and representations, which shall have no further force or effect. There are no agreements, conditions, understandings, promises, warranties, or representations, oral or written, express or implied, between the STATE and the CONTRACTOR other than as set forth or as referred to herein.
38. Severability. In the event that any provision of this Contract is declared invalid or unenforceable by a court, such invalidity or unenforceability shall not affect the validity or enforceability of the remaining terms of this Contract.
39. Waiver. The failure of the STATE to insist upon the strict compliance with any term, provision, or condition of this Contract shall not constitute or be deemed to constitute a waiver or relinquishment of the STATE'S right to enforce the same in accordance with this Contract. The fact that the STATE specifically refers to one provision of the procurement rules or one section of the Hawaii Revised Statutes, and does not include other provisions or statutory sections in this Contract shall not constitute a waiver or relinquishment of the STATE'S rights or the CONTRACTOR'S obligations under the procurement rules or statutes.
40. Pollution Control. If during the performance of this Contract, the CONTRACTOR encounters a "release" or a "threatened release" of a reportable quantity of a "hazardous substance," "pollutant," or "contaminant" as those terms are defined in section 128D-1, HRS, the CONTRACTOR shall immediately notify the STATE and all other appropriate state, county, or federal agencies as required by law. The Contractor shall take all necessary actions, including stopping work, to avoid causing, contributing to, or making worse a release of a hazardous substance, pollutant, or contaminant, and shall promptly obey any orders the Environmental Protection Agency or the state Department of Health issues in response to the release. In the event there is an ensuing cease-work period, and the STATE determines that this Contract requires an adjustment of the time for performance, the Contract shall be modified in writing accordingly.
41. Campaign Contributions. The CONTRACTOR is hereby notified of the applicability of 11-355, HRS, which states that campaign contributions are prohibited from specified state or county government contractors during the terms of their contracts if the contractors are paid with funds appropriated by a legislative body.
42. Confidentiality of Personal Information.
- a. Definitions.
- "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either name or data elements are not encrypted:
- (1) Social security number;
 - (2) Driver's license number or Hawaii identification card number; or

- (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial information.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Technological safeguards" means the technology and the policy and procedures for use of the technology to protect and control access to personal information.

b. Confidentiality of Material.

- (1) All material given to or made available to the CONTRACTOR by the STATE by virtue of this Contract which is identified as personal information, shall be safeguarded by the CONTRACTOR and shall not be disclosed without the prior written approval of the STATE.
- (2) CONTRACTOR agrees not to retain, use, or disclose personal information for any purpose other than as permitted or required by this Contract.
- (3) CONTRACTOR agrees to implement appropriate "technological safeguards" that are acceptable to the STATE to reduce the risk of unauthorized access to personal information.
- (4) CONTRACTOR shall report to the STATE in a prompt and complete manner any security breaches involving personal information.
- (5) CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect that is known to CONTRACTOR because of a use or disclosure of personal information by CONTRACTOR in violation of the requirements of this paragraph.
- (6) CONTRACTOR shall complete and retain a log of all disclosures made of personal information received from the STATE, or personal information created or received by CONTRACTOR on behalf of the STATE.

c. Security Awareness Training and Confidentiality Agreements.

- (1) CONTRACTOR certifies that all of its employees who will have access to the personal information have completed training on security awareness topics relating to protecting personal information.
- (2) CONTRACTOR certifies that confidentiality agreements have been signed by all of its employees who will have access to the personal information acknowledging that:
 - (A) The personal information collected, used, or maintained by the CONTRACTOR will be treated as confidential;
 - (B) Access to the personal information will be allowed only as necessary to perform the Contract; and
 - (C) Use of the personal information will be restricted to uses consistent with the services subject to this Contract.

d. Termination for Cause. In addition to any other remedies provided for by this Contract, if the STATE learns of a material breach by CONTRACTOR of this paragraph by CONTRACTOR, the STATE may at its sole discretion:

- (1) Provide an opportunity for the CONTRACTOR to cure the breach or end the violation; or
- (2) Immediately terminate this Contract.

In either instance, the CONTRACTOR and the STATE shall follow chapter 487N, HRS, with respect to notification of a security breach of personal information.

e. Records Retention.

- (1) Upon any termination of this Contract or as otherwise required by applicable law, CONTRACTOR shall, pursuant to chapter 487R, HRS, destroy all copies (paper or electronic form) of personal information received from the STATE.
- (2) The CONTRACTOR and any subcontractors shall maintain the files, books, and records that relate to the Contract, including any personal information created or received by the CONTRACTOR on behalf of the STATE, and any cost or pricing data, for at least three (3) years after the date of final payment under the Contract. The personal information shall continue to be confidential and shall only be disclosed as permitted or required by law. After the three (3) year, or longer retention period as required by law has ended, the files, books, and records that contain personal information shall be destroyed pursuant to chapter 487R, HRS or returned to the STATE at the request of the STATE.

SPECIAL PROVISIONS
(REQUIRED FEMA DISASTER PROVISIONS)
Updated 02/19/2026

Exhibit B

1. Administrative, Contractual, or Legal Remedies. For all contracts equal to or exceeding the Simplified Acquisition Threshold, set by the Civilian Acquisition Council and the Defense Acquisition Regulations Council pursuant to 48 CFR Part 2 and 41 U.S.C. 1908, Contractor agrees to be bound by the administrative, contractual, or legal remedies set forth in the State of Hawaii, General Conditions (AG-008), which govern contractors' violation or breach of contract terms and appropriate sanctions and penalties.
2. Termination for Cause and for Convenience. For all contracts in excess of \$10,000, Contractor agrees to be bound by the termination for cause and for convenience provisions set forth in the State of Hawaii, General Conditions (AG-008).
3. Equal Employment Opportunity. If this contract is for construction, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3, in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor." During the performance of this contract, the contractor agrees as follows:
 - A. The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.
 - B. The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.
 - C. The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.
 - D. The contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding,

SPECIAL PROVISIONS
(REQUIRED FEMA DISASTER PROVISIONS)
Updated 02/19/2026

Exhibit B

a notice to be provided advising the said labor union or workers' representatives of the contractor's commitments under section 202 of Executive Order 11246 of September 24, 1965, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

- E. The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.
 - F. The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.
 - G. In the event of the contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.
 - H. The contractor will include the portion of the sentence immediately preceding paragraph (3) and the provisions of paragraphs (A) through (G) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:
Provided, however, that in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the contractor may request the United States to enter into such litigation to protect the interests of the United States.
4. Davis-Bacon Act. If the Davis-Bacon Act, 40 U.S.C. §§ 3141–3148, is applicable to this Contract, the Contractor shall comply with all applicable provisions of the Act and shall pay all laborers and mechanics employed under this Contract wages at rates not less than those contained in the applicable wage determination issued by the U.S. Department of Labor and incorporated into this Contract. Such wages shall be paid not less frequently than once weekly, in accordance with 40 U.S.C. § 3142. The Contractor shall comply with the Copeland “Anti-Kickback” Act, 40 U.S.C. § 3145, and the U.S. Department of Labor regulations at 29 C.F.R. Parts 1, 3, and 5. The Contractor shall not induce, by any means, any person employed in the construction, prosecution, completion, or repair of public work to give up any part of the compensation to which the person is otherwise entitled. All suspected or reported violations of the Davis-Bacon Act or the Copeland Anti-Kickback Act shall be referred to the U.S. Department of Labor, Wage and Hour Division, in accordance with applicable federal requirements. The contractor shall include these labor standards provisions in all subcontracts at any tier and shall be responsible for compliance

SPECIAL PROVISIONS
(REQUIRED FEMA DISASTER PROVISIONS)
Updated 02/19/2026

Exhibit B

by any subcontractor or lower-tier subcontractor with all applicable Davis-Bacon and Copeland Act requirements.

5. Contract Work Hours and Safety Standards Act. If this contract in excess of \$100,000 and is subject to the Contract Work Hours and Safety Standards Act, 40 U.S.C. §§ 3701–3708, the Contractor shall comply with all applicable provisions of that Act and the U.S. Department of Labor regulations implementing it. Pursuant to 40 U.S.C. § 3702, the Contractor shall compute the wages of every laborer and mechanic employed on the Contract on the basis of a standard workweek of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.
6. Clean Air Act and Federal Water Pollution Control Act. Contractor agrees to comply with paragraph 40 (Pollution Control) of the State of Hawaii, General Conditions (AG-008), and all applicable standards, orders or regulations issued pursuant to the Clean Air Act, 42 U.S.C. §§ 7401-7671q, and the Federal Water Pollution Control Act, as amended, 33 U.S.C. §§ 1251-1387. Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).
7. Energy Efficiency. To the extent applicable to this contract, Contractor agrees to comply with all applicable mandatory standards and policies relating to energy efficiency of the State.
8. Excluded Parties List System. Contractor understands and agrees that if Contractor is listed on the government-wide Excluded Parties List System in the System for Award Management at www.SAM.gov as suspended or debarred, Contractor cannot be awarded this contract.
9. Byrd Anti-Lobbying Amendment. If this Contract is funded in whole or in part with federal funds and exceeds \$100,000, the Contractor shall comply with the requirements of 31 U.S.C. § 1352 and the implementing regulations at 31 C.F.R. Part 21. Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. §1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.
10. Recovered and Recycled Materials. To the extent applicable to this contract, Contractor agrees to comply with applicable requirements of 2 C.F.R. § 200.323.

SPECIAL PROVISIONS
(REQUIRED FEMA DISASTER PROVISIONS)
Updated 02/19/2026

Exhibit B

11. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment. To the extent applicable, Contractor agrees to comply with applicable requirements of 2 C.F.R. § 200.216.
12. Domestic Preferences for Procurements. To the extent applicable, Contractor agrees to comply with applicable requirements of 2 C.F.R. § 200.322.



Hawaii Electronic Information Technology Disability Access Standards

Published By: The Department of Accounting and General Services, Office of Enterprise
Technology Services, & the
Disability and Communication Access Board

Effective Date: April 20, 2026
Version 1.2

Revision History

Revision Number	Date	Revised By	Description of Changes
1.0	01/01/2025	ETS/DCAB	Initial release
1.1	01/22/2025	ETS/DCAB	Minor wording, diacritical mark, and formatting changes
1.2	04/21/2026	ETS/DCAB	DOJ compliance deadline updated to the extended date of April 26, 2027; corrected the effective date of DOJ rule; expanded hyperlinks for printability; minor appendix edits

Table of Contents

Purpose	2
Scope.....	2
Background	2
Authorities	3
Dates	3
Roles and Responsibilities.....	3
Functional Performance Criteria and Technical Requirements.....	4
Section 508 Standards	5
WCAG 2.1 Level A and AA	5
Exceptions	6
Section 508 E202 General Exceptions.....	6
DOJ Rule Exceptions.....	7
Accessibility Recommendations	8
Incorporate Accessibility Early in the IT Project Roadmapping and Planning Phases	8
Incorporate Accessibility in the Procurement Phase.....	8
Voluntary Product Accessibility Template (VPAT®)	8
Establish Monitoring and Reporting Mechanisms	9
Conduct Periodic Accessibility Reviews	9
Provide Training and Awareness.....	10
Continuously Improve.....	10
Definitions	10
References and Additional Resources	11
Appendix	13
Appendix C to Part 1194 – Functional Performance Criteria of Section 508 of the Rehabilitation Act .	13
Chapter 3: Functional Performance Criteria	13
Chapter 4: Hardware.....	14
Chapter 5: Software	20
Chapter 6: Support Documentation and Services	24
Chapter 7: Referenced Standards	24

Purpose

The State of Hawai'i is committed to providing individuals with disabilities access to electronic information technology (EIT) equivalent to access provided to individuals without disabilities.

The purpose of the Hawaii Electronic Information Technology Disability Access Standards, henceforth referred to as the Access Standards, is to establish minimum accessibility requirements to ensure that all electronic information technology developed, purchased, used, or provided by a state entity are made accessible to individuals with a disability.

Scope

These Access Standards apply to all state entities: the executive, legislative, and judicial branches of the State, including its departments, divisions, agencies, offices; public bodies; public elementary, secondary, and postsecondary schools; and the University of Hawai'i. State entities that contract with other entities to provide public service have an obligation to ensure that their contractors comply with these Access Standards.

These Access Standards apply to all EIT developed, purchased, used, or provided by a state entity, and all substantial modifications made by a state entity to EIT. Electronic information technology means electronic information, software, systems, and equipment used in the creation, manipulation, storage, display, or transmission of data, including: (1) Internet and intranet systems; (2) Websites and interfaces; (3) Software applications; (4) Operating systems; (5) Video and multimedia; (6) Telecommunication products; (7) Electronic and digital kiosks; (8) Information transaction machines; (9) Copiers and printers; and (10) Desktop and portable computers.

Background

Section 504 of the Rehabilitation Act of 1973 is a United States federal law that prohibits discrimination on the basis of disability in programs and activities that receive federal financial assistance.

Section 508 of the Rehabilitation Act requires federal agencies to make their electronic and information technology (EIT), also referred to as information and communication technology (ICT), accessible to people with disabilities. The law (29 U.S.C. § 794 (d)) applies to all federal agencies when they develop, procure, maintain, or use EIT. Under Section 508, access must be comparable to that available to employees and members of the public without disabilities.

The federal Americans with Disabilities Act (ADA) of 1990 extended anti-discrimination protections to various sectors beyond those covered by federal funding, including state and local governments. ADA Title II covers public services and accommodations.

Regulations issued by the U.S. Department of Justice (DOJ) on April 24, 2024, revised the ADA Title II regulations to specify that the Web Content Accessibility Guidelines (WCAG) Version 2.1, Level AA is the technical standard for state and local governments' web content and mobile apps.

In 2022, Hawai'i State Senate Bill 2144 was passed into law as Act 172, requiring the Office of Enterprise Technology Services, in consultation with the Disability and Communication Access Board and a working group composed of stakeholders, to develop and publish electronic information technology (EIT) accessibility standards to be implemented by all state entities.

The accessibility standards, referred to as the Hawaii Electronic Information Technology Disability Access Standards, shall require that all electronic information technology developed, purchased, used, or provided by a state entity be made accessible to individuals with a disability, consistent with federal standards to implement section 508 of the Rehabilitation Act of 1973, as amended, and the web access standards issued by the World Wide Web Consortium Web Accessibility Initiative, including functional performance criteria and technical requirements for accessibility.

Authorities

- A. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d)
<https://www.govinfo.gov/content/pkg/USCODE-2011-title29/html/USCODE-2011-title29-chap16-subchapV-sec794d.htm>
- B. Americans with Disabilities Act of 1990, As Amended (42 U.S.C. §§ 12101–12213)
<https://www.ada.gov/law-and-regs/ada/>
- C. Act 172, Session Laws of Hawai‘i 2022 – Relating to Electronic Information Technology Accessibility for Persons with Disabilities
https://www.capitol.hawaii.gov/sessions/session2022/bills/GM1273_.PDF
- D. DOJ Rule, Nondiscrimination on the Basis of Disability; Accessibility of Web Information and Services of State and Local Government Entities (28 C.F.R. Part 35 Subpart H)
<https://www.ecfr.gov/current/title-28/chapter-I/part-35/subpart-H/section-35.200>

Dates

Effective Date of DOJ Rule: June 24, 2024.

Effective Date of DOJ Interim Final Rule: April 20, 2026.

Extension of Compliance Date: In accordance with 28 C.F.R. § 35.200 (DOJ Rule), a public entity with a total population of 50,000 or more shall ensure compliance with DOJ Interim Final Rule by April 26, 2027 (extended from April 24, 2026).

DOJ Rule, 28 C.F.R. § 35.200 Requirements for web and mobile accessibility:

<https://www.ecfr.gov/current/title-28/chapter-I/part-35/subpart-H/section-35.200>

DOJ Interim Final Rule on Extension of Compliance Date:

<https://www.federalregister.gov/documents/2026/04/20/2026-07663/extension-of-compliance-dates-for-nondiscrimination-on-the-basis-of-disability-accessibility-of-web>

Roles and Responsibilities

- A. The Office of Enterprise Technology Services (ETS) Chief Information Officer (CIO):
 - a. Oversees development and publication of the Hawaii Electronic Information Technology Disability Access Standards.
 - b. Provides vision and direction for ensuring that electronic information technology (EIT) developed, purchased, used, or provided by a state entity is accessible to individuals with a disability.

- c. Reviews the Access Standards every three years after the date of initial publication, or more frequently if deemed necessary by the ETS CIO, and amends the Access Standards to reflect advances or changes in electronic information technology.
- B. The Disability and Communication Access Board (DCAB):
 - a. Provides ETS CIO consultation to develop and publish the Access Standards.
 - b. Provides ETS CIO consultation to carry out the triennial Access Standards review and amendments.
 - c. Provides guidance to state agencies regarding the Access Standards.
- C. Department/Agency Director (or equivalent or designee):
 - a. No later than 6 months after publication of the Access Standards, review the Access Standards and revise their department's/agency's procurement and development rules, policies, and procedures to incorporate the Access Standards.
 - b. No later than 6 months after the publication of any amendment, review the Access Standards and revise their department's/agency's procurement and development rules, policies, and procedures to incorporate the Access Standards.
 - c. Ensure conformance to the Access Standards.
 - d. Ensure the relevant Access Standards compliance language is included in all contractual actions for electronic information technology items and services.
- D. Department/Agency ADA Coordinators:
 - a. Receive and process grievances alleging discrimination on the basis of disability.
- E. Department/Agency EEO Officer (or equivalent):
 - a. Receive and process employee grievances alleging discrimination on the basis of disability.

Functional Performance Criteria and Technical Requirements

Act 172, Session Laws of Hawai'i (SLH) 2022, requires the Access Standards to be consistent with (1) accessibility standards issued by the United States Access Board which implement Section 508 of the Rehabilitation Act of 1973, as amended, and (2) web access standards issued by the World Wide Web Consortium Web Accessibility Initiative.

All electronic information technology that is procured, developed, maintained, or used by state entities shall conform to the following:

- A. Section 508 Standards (36 C.F.R. Part 1194)
 - a. Appendix A to 36 C.F.R. Part 1194 – Section 508 of the Rehabilitation Act: Application and Scoping Requirements
<https://www.access-board.gov/ict/#E101-general>
 - b. Appendix C to Part 1194 – Functional Performance Criteria and Technical Requirements
<https://www.access-board.gov/ict/#301-general>
- B. Web Content Accessibility Guidelines (WCAG) 2.1 Level A and AA
 (<https://www.w3.org/TR/WCAG21/>) or a subsequent version as adopted by the United States Access Board or Department of Justice.

Section 508 Standards

Under Section 508 of the Rehabilitation Act of 1973, as amended, federal agencies must provide individuals with disabilities, including employees and members of the public, access to information comparable to access available to others.

The functional performance criteria under Section 508 are as follows:

- **Without Vision:** Where a visual mode of operation is provided, information and communication technology (ICT) shall provide at least one mode of operation that does not require user vision.
- **With Limited Vision:** Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited vision.
- **Without Perception of Color:** Where a visual mode of operation is provided, ICT shall provide at least one visual mode of operation that does not require user perception of color.
- **Without Hearing:** Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that does not require user hearing.
- **With Limited Hearing:** Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited hearing.
- **Without Speech:** Where speech is used for input, control, or operation, ICT shall provide at least one mode of operation that does not require user speech.
- **With Limited Manipulation:** Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that does not require fine motor control or simultaneous manual operations.
- **With Limited Reach and Strength:** Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that is operable with limited reach and limited strength.
- **With Limited Language, Cognitive, and Learning Abilities:** ICT shall provide features making its use by individuals with limited cognitive, language, and learning abilities simpler and easier.

Please refer to the Appendix for a full extract of *Appendix C to Part 1194—Functional Performance Criteria and Technical Requirements* of the Section 508 of the Rehabilitation Act.

WCAG 2.1 Level A and AA

The WCAG 2.1 Level A and AA will make web content more accessible to people with disabilities, including people with visual, auditory, physical, speech, cognitive, language, learning, and neurological disabilities. Although WCAG 2.1 Level A and AA cover a wide range of issues, they are not able to address the needs of people with all types, degrees, and combinations of disability. WCAG 2.1 Level A and AA also make web content more usable by older individuals with changing abilities due to aging and often improve usability for users in general.

The basic principles that lay the foundation necessary for anyone to access and use web content are as follows:

1. **Perceivable** - Information and user interface components must be presentable to users in ways users can perceive.
 - This means that users must be able to perceive the information being presented (it cannot be invisible to all of their senses).
2. **Operable** - User interface components and navigation must be operable.

- This means that users must be able to operate the interface (the interface cannot require interaction that a user cannot perform).
- 3. **Understandable** - Information and the operation of user interface must be understandable.
 - This means that users must be able to understand the information as well as the operation of the user interface (the content or operation cannot be beyond their understanding).
- 4. **Robust** - Content must be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies.
 - This means that users must be able to access the content as technologies advance (as technologies and user agents evolve, the content should remain accessible).

Exceptions

Electronic information technology (EIT) may be exempt from the Disability Access Standards as specified by the U.S. Access Board at the following website: <https://www.access-board.gov/ict/#E202-general-exceptions>. Exceptions applicable at the federal level apply to the state with the implementation of the Access Standards.

The Access Standards shall not require the installation of specific accessibility-related software or peripheral devices at the workstation of an employee who is not an individual with a disability; the Access Standards require all workstation technology used by a state entity to be compatible with accessibility-related software and peripheral devices.

Section 508 E202 General Exceptions

- **E202.1 General** – Information and communication technology (ICT) shall be exempt from compliance with the Revised 508 Standards to the extent specified by E202.
- **E202.2 Legacy ICT** – Any component or portion of existing ICT that complies with an earlier standard issued pursuant to Section 508 of the Rehabilitation Act of 1973, as amended (as republished in Appendix D), and that has not been altered on or after January 18, 2018, shall not be required to be modified to conform to the Revised 508 Standards.
- **E202.3 National Security Systems** – The Revised 508 Standards do not apply to ICT operated by agencies as part of a national security system, as defined by 40 U.S.C. 11103(a).
- **E202.4 Federal Contracts** – ICT acquired by a contractor incidental to a contract shall not be required to conform to the Revised 508 Standards.
- **E202.5 ICT Functions Located in Maintenance or Monitoring Spaces** – Where status indicators and operable parts for ICT functions are located in spaces that are frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment, such status indicators and operable parts shall not be required to conform to the Revised 508 Standards.
- **E202.6 Undue Burden or Fundamental Alteration** – Where an agency determines in accordance with E202.6 that conformance to requirements in the Revised 508 Standards would impose an undue burden or would result in a fundamental alteration in the nature of the ICT, conformance shall be required only to the extent that it does not impose an undue burden, or result in a fundamental alteration in the nature of the ICT.
- **E202.6.1 Basis for a Determination of Undue Burden** – In determining whether conformance to requirements in the Revised 508 Standards would impose an undue burden on the agency, the

agency shall consider the extent to which conformance would impose significant difficulty or expense considering the agency resources available to the program or component for which the ICT is to be procured, developed, maintained, or used.

- **E202.6.2 Required Documentation** – The responsible agency official shall document in writing the basis for determining that conformance to requirements in the Revised 508 Standards constitute an undue burden on the agency, or would result in a fundamental alteration in the nature of the ICT. The documentation shall include an explanation of why and to what extent compliance with applicable requirements would create an undue burden or result in a fundamental alteration in the nature of the ICT.
- **E202.6.3 Alternative Means** – Where conformance to one or more requirements in the Revised 508 Standards imposes an undue burden or a fundamental alteration in the nature of the ICT, the agency shall provide individuals with disabilities access to and use of information and data by an alternative means that meets identified needs.
- **E202.7 Best Meets** – Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs.
- **E202.7.1 Required Documentation** – The responsible agency official shall document in writing: (a) the non-availability of conforming ICT, including a description of market research performed and which provisions cannot be met, and (b) the basis for determining that the ICT to be procured best meets the requirements in the Revised 508 Standards consistent with the agency's business needs.
- **E202.7.2 Alternative Means** – Where ICT that fully conforms to the Revised 508 Standards is not commercially available, the agency shall provide individuals with disabilities access to and use of information and data by an alternative means that meets identified needs.

DOJ Rule Exceptions

The requirements of 28 C.F.R. § 35.200 do not apply to the following:

- A. **Archived web content** - Archived web content as defined in 28 C.F.R. § 35.104.
- B. **Preexisting conventional electronic documents** - Conventional electronic documents that are available as part of a public entity's web content or mobile apps before the date the public entity is required to comply with this subpart, unless such documents are currently used to apply for, gain access to, or participate in the public entity's services, programs, or activities.
- C. **Content posted by a third party** - Content posted by a third party, unless the third party is posting due to contractual, licensing, or other arrangements with the public entity.
- D. **Individualized, password-protected or otherwise secured conventional electronic documents.** Conventional electronic documents that are:
 - 1. About a specific individual, their property, or their account; and
 - 2. Password-protected or otherwise secured.
- E. **Preexisting social media posts** - A public entity's social media posts that were posted before the date the public entity is required to comply with this subpart.

28 C.F.R. § 35.201 Exceptions:

<https://www.ecfr.gov/current/title-28/chapter-I/part-35/subpart-H/section-35.201>

28 C.F.R. § 35.104 Definition of Archived web content:

<https://www.ecfr.gov/current/title-28/chapter-I/part-35/subpart-A/section-35.104>

Accessibility Recommendations

The best strategy to address accessibility compliance involves a comprehensive and proactive approach, which includes planning and accessibility testing throughout the product lifecycle. To ensure that state entities implement the accessibility standards, the following recommendations for planning, reporting, monitoring, and enforcement should be considered.

Incorporate Accessibility Early in the IT Project Roadmapping and Planning Phases

State entities must consider the Access Standards in all IT project plans that include an investment in new or existing electronic information technology.

- Accessibility requirements must be included in the project specifications of new systems, especially in the modernization of major systems, and be evaluated throughout any major enhancements of existing systems during the design and development phases.
- Governing IT entities and/or IT management shall provide reference to the Access Standards to the state entities during IT governance roadmapping and planning phases for IT projects.

Incorporate Accessibility in the Procurement Phase

No later than six months after the publication of the Access Standards, each state entity shall review the standards and revise the entity's existing procurement rules, policies, and procedures to incorporate the standards.

- To ensure compliance, state entities shall include a requirement similar to the following whenever procuring information technology:

All electronic information technology developed or provided under this contract or procurement shall comply with the applicable requirements of the Hawaii Electronic Information Technology Disability Access Standards (Access Standards).

- State entities must clearly communicate the expectation that vendors and contractors are held to the Access Standards.
- State entities shall keep documentation of their accessibility evaluation and selection criteria for the evaluation of proposals.
- Where applicable, the vendor shall provide the state entity with its most recent Accessibility Conformance Report (ACR).

Voluntary Product Accessibility Template (VPAT®)

A Voluntary Product Accessibility Template (VPAT®) (<https://www.section508.gov/sell/acr/>) is a document that explains how information and communication technology (ICT) products such as software, hardware, electronic content, and support documentation meet (conform to) the Revised 508 Standards for IT accessibility. VPAT® helps Federal agency contracting officials and government buyers to assess ICT for accessibility when doing market research and evaluating proposals.

Government solicitations which include ICT will specify accessibility requirements, indicating which provisions are required to ensure the deliverable is accessible. A VPAT® is a good way to address the accessibility requirements defined in the solicitation.

Establish Monitoring and Reporting Mechanisms

Implement a system for ongoing monitoring of EIT accessibility and establish reporting mechanisms that can show conformance status over time.

- **Automated Accessibility Testing and Reporting:** Implement automated accessibility testing tools that can scan state websites, applications, and documents for common accessibility issues. These tools can help identify potential problems without requiring extensive manual effort.
 - Acquire access to the Siteimprove - <https://siteimprove.com/en-us/content-accessibility/> automated evaluation tool via ETS. The state has a license to use Siteimprove for all Hawaii.gov websites.
- **Compliance Reporting:** Establish a system for agencies and departments to regularly report on their compliance with accessibility standards. This involves documenting efforts made, progress achieved, and any identified challenges or areas for improvement.
- **Complaint and Grievance Process:** Develop and publish grievance procedures to allow anyone who wishes to file a complaint alleging discrimination on the basis of disability in violation of the standards set forth in the Access Standards. Identify an entity resource, such as an agency ADA Coordinator or EEO Officer to manage the complaints and ensure fair and prompt resolution.

Conduct Periodic Accessibility Reviews

State entities shall perform regular accessibility audits and testing throughout the product lifecycle, identify issues for review and remediation, evaluate the impact and risk of each issue to appropriately prioritize remediation efforts, and to iteratively improve the conformance levels of the EIT.

- **Accessibility Audits:** Leverage automated testing tools to generate periodic accessibility reports.
 - To get started with website content accessibility evaluation, the departmental content creators can first use the W3C-provided Easy Checks preliminary evaluation procedure, explained at <https://www.w3.org/WAI/test-evaluate/preliminary/>. This preliminary procedure is particularly useful for content creators with no prior experience in authoring accessible web content.
 - Incorporating hands-on testing by individuals with disabilities into the digital accessibility process adds significant value by providing real-world insights that automated tools or theoretical reviews may overlook. This inclusive approach ensures that digital products are truly usable for all people, not just technically compliant. By involving individuals with diverse disabilities in testing, state entities can better understand the challenges they face and validate the compatibility of our products with various assistive technologies like screen readers or voice control systems. Ultimately, this leads to more user-centered designs, a stronger commitment to accessibility, and improved overall user experience for everyone.
- **Compliance Reviews:** State entities must report the level of conformance of EIT systems to their governing IT entities or IT management so that accessibility conformance can be tracked and analyzed.

- **Accessibility Remediation Plans:** Create a plan to address accessibility issues identified within audits, reviews, and reports and prioritize the high-risk issues.

Provide Training and Awareness

- Encourage accessibility training for acquisition professionals, IT project managers, communications staff, web managers, software developers, and authors of digital content.
- Accessibility statements adhering to the Access Standards shall be made available, where appropriate, on state entity websites. Each entity shall craft a message highlighting the agency's commitment to ensuring equivalent access to information for people with disabilities, and include a reference to the Access Standards, a program point of contact or a method to request assistance or provide feedback, and the date the statement was last updated.

Continuously Improve

- **Periodic review of the Access Standards:** ETS, in consultation with DCAB, shall review the accessibility standards every three years after the date of the initial publication, or more frequently if the Chief Information Officer deems it necessary, and amend the standards to reflect advances or changes in electronic information technology. Within six months of the publication of any amended accessibility standards, each state entity shall review the amended standards and shall revise the entity's existing procurement and development rules, policies, and procedures to incorporate the amended standards accordingly.
- **User Feedback Mechanisms:** Set up mechanisms for users, including individuals with disabilities, to provide feedback on the accessibility of state websites, applications, and services. This may involve implementing feedback forms, contact information, or dedicated accessibility service centers. Monitoring and responding to user feedback may require a moderate amount of labor, but is crucial for gathering valuable insights.
- **Engage with the Accessibility Community:** Involve individuals with disabilities, disability advocacy groups, and accessibility experts in the design, development, and testing phases. Their insights and feedback are invaluable for identifying accessibility barriers, ensuring that the EIT is truly inclusive, and that the state's efforts are meeting the needs of the community.

Definitions

Accessibility - means the ability of an individual with a disability to receive, use, and manipulate data and operate controls included in electronic information technology in a manner equivalent to that of individuals who do not have disabilities.

Accessibility Conformance Report (ACR) - is a document that formally summarizes the extent to which an information and communications technology (ICT) product or service conforms to an agreed set of international accessibility guidelines and standards.

Electronic Information - is information that is created, stored, transmitted, or processed in an electronic format. This can include, but is not limited to:

- (1) Electronic documents, files, and data;
- (2) Emails, text messages, and faxes;
- (3) Databases, spreadsheets, and programs;
- (4) Image, sound, and video files; and

- (5) Web pages and information submitted online.

Electronic Information Technology (EIT) - also referred to as information and communication technology (ICT) as defined by Section 508 (<https://www.access-board.gov/ict/#E103-definitions>) means electronic information, software, systems, and equipment used in the creation, manipulation, storage, display, or transmission of data, including:

- (1) Internet and intranet systems;
- (2) Websites and interfaces;
- (3) Software applications;
- (4) Operating systems;
- (5) Video and multimedia;
- (6) Telecommunication products;
- (7) Electronic and digital kiosks;
- (8) Information transaction machines;
- (9) Copiers and printers; and
- (10) Desktop and portable computers.

Individual with a disability - means an individual with impairments that limit the individual's ability to access or use electronic information technology, including an individual who has:

- (1) No or limited vision;
- (2) No or limited hearing;
- (3) Physical disabilities; or
- (4) Cognitive impairment

State entity - means the executive, legislative, and judicial branches of the State, including its departments, divisions, agencies, offices; public bodies; public elementary, secondary, and postsecondary schools; and the University of Hawai'i.

References and Additional Resources

- U.S. General Services Administration (GSA) IT Accessibility Laws and Policies
<https://www.section508.gov/manage/laws-and-policies/>
- Accessibility of Web Content and Mobile Apps Provided by State and Local Government Entities: A Small Entity Compliance Guide
<https://www.ada.gov/resources/small-entity-compliance-guide/>
- PDFs Authoring Guides
<https://www.section508.gov/create/pdfs/authoring-guides/>
- ICT Testing Baseline for Electronic Documents
<https://ictbaseline.access-board.gov/document-baselines/>
- Create Accessible Meetings
<https://www.section508.gov/create/accessible-meetings/>
- Mapping of WCAG 2.0 to Functional Performance Criteria
<https://www.section508.gov/develop/mapping-wcag-to-fpc/>
- What's New in WCAG 2.1
<https://www.w3.org/WAI/standards-guidelines/wcag/new-in-21/>

- Developing a Website Accessibility Statement
<https://www.section508.gov/manage/laws-and-policies/website-accessibility-statement/>

Appendix

Appendix C to Part 1194 – Functional Performance Criteria of Section 508 of the Rehabilitation Act

The functional performance criteria provided below are an extract from *Appendix C to Part 1194—Functional Performance Criteria and Technical Requirements* of Section 508 of the Rehabilitation Act.

Source: <https://www.ecfr.gov/current/title-36/chapter-XI/part-1194/appendix-Appendix%20C%20to%20Part%201194>

Chapter 3: Functional Performance Criteria

301 General

- **301.1 Scope.** The requirements of Chapter 3 shall apply to ICT where required by Chapter 2 (Scoping Requirements) and where otherwise referenced in any other chapter of these Standards.

302 Functional Performance Criteria

- **302.1 Without Vision.** Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that does not require user vision.
- **302.2 With Limited Vision.** Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited vision.
- **302.3 Without Perception of Color.** Where a visual mode of operation is provided, ICT shall provide at least one visual mode of operation that does not require user perception of color.
- **302.4 Without Hearing.** Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that does not require user hearing.
- **302.5 With Limited Hearing.** Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited hearing.
- **302.6 Without Speech.** Where speech is used for input, control, or operation, ICT shall provide at least one mode of operation that does not require user speech.
- **302.7 With Limited Manipulation.** Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that does not require fine motor control or simultaneous manual operations.
- **302.8 With Limited Reach and Strength.** Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that is operable with limited reach and limited strength.
- **302.9 With Limited Language, Cognitive, and Learning Abilities.** ICT shall provide features making its use by individuals with limited cognitive, language, and learning abilities simpler and easier.

Chapter 4: Hardware

401 General

- **401.1 Scope.** The requirements of Chapter 4 shall apply to ICT that is hardware where required by Chapter 2 (Scoping Requirements) and where otherwise referenced in any other chapter of these Standards.
 - **EXCEPTION:** Hardware that is assistive technology shall not be required to conform to the requirements of this chapter.

402 Closed Functionality

- **402.1 General.** ICT with closed functionality shall be operable without requiring the user to attach or install assistive technology other than personal headsets or other audio couplers, and shall conform to 402.
- **402.2 Speech-Output Enabled.** ICT with a display screen shall be speech-output enabled for full and independent use by individuals with vision impairments.
 - **EXCEPTIONS:**
 1. Variable message signs conforming to 402.5 shall not be required to be speech-output enabled.
 2. Speech output shall not be required where ICT display screens only provide status indicators and those indicators conform to 409.
 3. Where speech output cannot be supported due to constraints in available memory or processor capability, ICT shall be permitted to conform to 409 in lieu of 402.2.
 4. Audible tones shall be permitted instead of speech output where the content of user input is not displayed as entered for security purposes, including, but not limited to, asterisks representing personal identification numbers.
 5. Speech output shall not be required for: The machine location; date and time of transaction; customer account number; and the machine identifier or label.
 6. Speech output shall not be required for advertisements and other similar information unless they convey information that can be used for the transaction being conducted.
 - **402.2.1 Information Displayed On-Screen.** Speech output shall be provided for all information displayed on-screen.
 - **402.2.2 Transactional Outputs.** Where transactional outputs are provided, the speech output shall audibly provide all information necessary to verify a transaction.
 - **402.2.3 Speech Delivery Type and Coordination.** Speech output shall be delivered through a mechanism that is readily available to all users, including, but not limited to, an industry standard connector or a telephone handset. Speech shall be recorded or

digitized human, or synthesized. Speech output shall be coordinated with information displayed on the screen.

- **402.2.4 User Control.** Speech output for any single function shall be automatically interrupted when a transaction is selected. Speech output shall be capable of being repeated and paused.
- **402.2.5 Braille Instructions.** Where speech output is required by 402.2, braille instructions for initiating the speech mode of operation shall be provided. Braille shall be contracted and shall conform to 36 CFR part 1191, Appendix D, Section 703.3.1.
 - **EXCEPTION:** Devices for personal use shall not be required to conform to 402.2.5.
- **402.3 Volume.** ICT that delivers sound, including speech output required by 402.2, shall provide volume control and output amplification conforming to 402.3.
 - **EXCEPTION:** ICT conforming to 412.2 shall not be required to conform to 402.3.
 - **402.3.1 Private Listening.** Where ICT provides private listening, it shall provide a mode of operation for controlling the volume. Where ICT delivers output by an audio transducer typically held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.
 - **402.3.2 Non-private Listening.** Where ICT provides non-private listening, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. A function shall be provided to automatically reset the volume to the default level after every use.
- **402.4 Characters on Display Screens.** At least one mode of characters displayed on the screen shall be in a sans serif font. Where ICT does not provide a screen enlargement feature, characters shall be 3/16 inch (4.8 mm) high minimum based on the uppercase letter "I". Characters shall contrast with their background with either light characters on a dark background or dark characters on a light background.
- **402.5 Characters on Variable Message Signs.** Characters on variable message signs shall conform to section 703.7 Variable Message Signs of ICC A117.1-2009 (incorporated by reference, see 702.6.1).

403 Biometrics

- **403.1 General.** Where provided, biometrics shall not be the only means for user identification or control.
 - **EXCEPTION:** Where at least two biometric options that use different biological characteristics are provided, ICT shall be permitted to use biometrics as the only means for user identification or control.

404 Preservation of Information Provided for Accessibility

- **404.1 General.** ICT that transmits or converts information or communication shall not remove non-proprietary information provided for accessibility or shall restore it upon delivery.

405 Privacy

- **405.1 General.** The same degree of privacy of input and output shall be provided to all individuals. When speech output required by 402.2 is enabled, the screen shall not blank automatically.

406 Standard Connections

- **406.1 General.** Where data connections used for input and output are provided, at least one of each type of connection shall conform to industry standard non-proprietary formats.

407 Operable Parts

- **407.1 General.** Where provided, operable parts used in the normal operation of ICT shall conform to 407.
- **407.2 Contrast.** Where provided, keys and controls shall contrast visually from background surfaces. Characters and symbols shall contrast visually from background surfaces with either light characters or symbols on a dark background or dark characters or symbols on a light background.
- **407.3 Input Controls.** At least one input control conforming to 407.3 shall be provided for each function.
 - **EXCEPTION:** Devices for personal use with input controls that are audibly discernible without activation and operable by touch shall not be required to conform to 407.3.
 - **407.3.1 Tactilely Discernible.** Input controls shall be operable by touch and tactilely discernible without activation.
 - **407.3.2 Alphabetic Keys.** Where provided, individual alphabetic keys shall be arranged in a QWERTY-based keyboard layout and the "F" and "J" keys shall be tactilely distinct from the other keys.
 - **407.3.3 Numeric Keys.** Where provided, numeric keys shall be arranged in a 12-key ascending or descending keypad layout. The number five key shall be tactilely distinct from the other keys. Where the ICT provides an alphabetic overlay on numeric keys, the relationships between letters and digits shall conform to ITU-T Recommendation E.161 (incorporated by reference, see 702.7.1).
- **407.4 Key Repeat.** Where a keyboard with key repeat is provided, the delay before the key repeat feature is activated shall be fixed at, or adjustable to, 2 seconds minimum.
- **407.5 Timed Response.** Where a timed response is required, the user shall be alerted visually, as well as by touch or sound, and shall be given the opportunity to indicate that more time is needed.
- **407.6 Operation.** At least one mode of operation shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate operable parts shall be 5 pounds (22.2 N) maximum.

- **407.7 Tickets, Fare Cards, and Keycards.** Where tickets, fare cards, or keycards are provided, they shall have an orientation that is tactilely discernible if orientation is important to further use of the ticket, fare card, or keycard.
- **407.8 Reach Height and Depth.** At least one of each type of operable part of stationary ICT shall be at a height conforming to 407.8.2 or 407.8.3 according to its position established by the vertical reference plane specified in 407.8.1 for a side reach or a forward reach. Operable parts used with speech output required by 402.2 shall not be the only type of operable part complying with 407.8 unless that part is the only operable part of its type.
 - **407.8.1 Vertical Reference Plane.** Operable parts shall be positioned for a side reach or a forward reach determined with respect to a vertical reference plane. The vertical reference plane shall be located in conformance to 407.8.2 or 407.8.3.
 - **407.8.1.1 Vertical Plane for Side Reach.** Where a side reach is provided, the vertical reference plane shall be 48 inches (1220 mm) long minimum.
 - **407.8.1.2 Vertical Plane for Forward Reach.** Where a forward reach is provided, the vertical reference plane shall be 30 inches (760 mm) long minimum.
 - **407.8.2 Side Reach.** Operable parts of ICT providing a side reach shall conform to 407.8.2.1 or 407.8.2.2. The vertical reference plane shall be centered on the operable part and placed at the leading edge of the maximum protrusion of the ICT within the length of the vertical reference plane. Where a side reach requires a reach over a portion of the ICT, the height of that portion of the ICT shall be 34 inches (865 mm) maximum.
 - **407.8.2.1 Unobstructed Side Reach.** Where the operable part is located 10 inches (255 mm) or less beyond the vertical reference plane, the operable part shall be 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor.
 - **407.8.2.2 Obstructed Side Reach.** Where the operable part is located more than 10 inches (255 mm), but not more than 24 inches (610 mm), beyond the vertical reference plane, the height of the operable part shall be 46 inches (1170 mm) high maximum and 15 inches (380 mm) high minimum above the floor. The operable part shall not be located more than 24 inches (610 mm) beyond the vertical reference plane.
 - **407.8.3 Forward Reach.** Operable parts of ICT providing a forward reach shall conform to 407.8.3.1 or 407.8.3.2. The vertical reference plane shall be centered, and intersect with, the operable part. Where a forward reach allows a reach over a portion of the ICT, the height of that portion of the ICT shall be 34 inches (865 mm) maximum.
 - **407.8.3.1 Unobstructed Forward Reach.** Where the operable part is located at the leading edge of the maximum protrusion within the length of the vertical reference plane of the ICT, the operable part shall be 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor.

- **407.8.3.2 Obstructed Forward Reach.** Where the operable part is located beyond the leading edge of the maximum protrusion within the length of the vertical reference plane, the operable part shall conform to 407.8.3.2. The maximum allowable forward reach to an operable part shall be 25 inches (635 mm).
- **407.8.3.2.1 Operable Part Height for ICT with Obstructed Forward Reach.** The height of the operable part shall conform to Table 407.8.3.2.1.

Table 407.8.3.2.1 - Operable Part Height for ICT With Obstructed Forward Reach

Reach depth	Operable part height
Less than 20 inches (510 mm)	48 inches (1220 mm) maximum.
20 inches (510 mm) to 25 inches (635 mm)	44 inches (1120 mm) maximum.

- **407.8.3.2.2 Knee and Toe Space under ICT with Obstructed Forward Reach.** Knee and toe space under ICT shall be 27 inches (685 mm) high minimum, 25 inches (635 mm) deep maximum, and 30 inches (760 mm) wide minimum and shall be clear of obstructions.
 - **EXCEPTIONS:**
 1. Toe space shall be permitted to provide a clear height of 9 inches (230 mm) minimum above the floor and a clear depth of 6 inches (150 mm) maximum from the vertical reference plane toward the leading edge of the ICT.
 2. At a depth of 6 inches (150 mm) maximum from the vertical reference plane toward the leading edge of the ICT, space between 9 inches (230 mm) and 27 inches (685 mm) minimum above the floor shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for every 6 inches (150 mm) in height.

408 Display Screens

- **408.1 General.** Where provided, display screens shall conform to 408.
- **408.2 Visibility.** Where stationary ICT provides one or more display screens, at least one of each type of display screen shall be visible from a point located 40 inches (1015 mm) above the floor space where the display screen is viewed.

- **408.3 Flashing.** Where ICT emits lights in flashes, there shall be no more than three flashes in any one-second period.
 - **EXCEPTION:** Flashes that do not exceed the general flash and red flash thresholds defined in WCAG 2.1 (incorporated by reference, *see* 702.10.1) are not required to conform to 408.3.

409 Status Indicators

- **409.1 General.** Where provided, status indicators shall be discernible visually and by touch or sound.

410 Color Coding

- **410.1 General.** Where provided, color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

411 Audible Signals

- **411.1 General.** Where provided, audible signals or cues shall not be used as the only means of conveying information, indicating an action, or prompting a response.

412 ICT With Two-Way Voice Communication

- **412.1 General.** ICT that provides two-way voice communication shall conform to 412.
- **412.2 Volume Gain.** ICT that provides two-way voice communication shall conform to 412.2.1 or 412.2.2.
 - **412.2.1 Volume Gain for Wireline Telephones.** Volume gain conforming to 47 CFR 68.317 shall be provided on analog and digital wireline telephones.
 - **412.2.2 Volume Gain for Non-Wireline ICT.** A method for increasing volume shall be provided for non-wireline ICT.
- **412.3 Interference Reduction and Magnetic Coupling.** Where ICT delivers output by a handset or other type of audio transducer that is typically held up to the ear, ICT shall reduce interference with hearing technologies and provide a means for effective magnetic wireless coupling in conformance with 412.3.1 or 412.3.2.
 - **412.3.1 Wireless Handsets.** ICT in the form of wireless handsets shall conform to ANSI/IEEE C63.19-2011 (incorporated by reference, *see* 702.5.1).
 - **412.3.2 Wireline Handsets.** ICT in the form of wireline handsets, including cordless handsets, shall conform to TIA-1083-B (incorporated by reference, *see* 702.9.1).
- **412.4 Digital Encoding of Speech.** ICT in IP-based networks shall transmit and receive speech that is digitally encoded in the manner specified by ITU-T Recommendation G.722.2 (incorporated by reference, *see* 702.7.2) or IETF RFC 6716 (incorporated by reference, *see* 702.8.1).
- **412.5 Real-Time Text Functionality.** [Reserved].
- **412.6 Caller ID.** Where provided, caller identification and similar telecommunications functions shall be visible and audible.

- **412.7 Video Communication.** Where ICT provides real-time video functionality, the quality of the video shall be sufficient to support communication using sign language.

413 Closed Caption Processing Technologies

- **413.1 General.** Where ICT displays or processes video with synchronized audio, ICT shall provide closed caption processing technology that conforms to 413.1.1 or 413.1.2.
 - **413.1.1 Decoding and Display of Closed Captions.** Players and displays shall decode closed caption data and support display of captions.
 - **413.1.2 Pass-Through of Closed Caption Data.** Cabling and ancillary equipment shall pass through caption data.

414 Audio Description Processing Technologies

- **414.1 General.** Where ICT displays or processes video with synchronized audio, ICT shall provide audio description processing technology conforming to 414.1.1 or 414.1.2.
 - **414.1.1 Digital Television Tuners.** Digital television tuners shall provide audio description processing that conforms to ATSC A/53 Digital Television Standard, Part 5 (2014) (incorporated by reference, see 702.2.1). Digital television tuners shall provide processing of audio description when encoded as a Visually Impaired (VI) associated audio service that is provided as a complete program mix containing audio description according to the ATSC A/53 standard.
 - **414.1.2 Other ICT.** ICT other than digital television tuners shall provide audio description processing.

415 User Controls for Captions and Audio Descriptions

- **415.1 General.** Where ICT displays video with synchronized audio, ICT shall provide user controls for closed captions and audio descriptions conforming to 415.1.
 - **EXCEPTION:** Devices for personal use shall not be required to conform to 415.1 provided that captions and audio descriptions can be enabled through system-wide platform settings.
 - **415.1.1 Caption Controls.** Where ICT provides operable parts for volume control, ICT shall also provide operable parts for caption selection.
 - **415.1.2 Audio Description Controls.** Where ICT provides operable parts for program selection, ICT shall also provide operable parts for the selection of audio description.

Chapter 5: Software

501 General

- **501.1 Scope.** The requirements of Chapter 5 shall apply to software where required by Chapter 2 (Scoping Requirements) and where otherwise referenced in any other chapter of these Standards.
 - **EXCEPTION:** Where Web applications do not have access to platform accessibility services and do not include components that have access to platform accessibility

services, they shall not be required to conform to 502 or 503 provided that they conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.1 (incorporated by reference, see 702.10.1).

502 Interoperability With Assistive Technology

- **502.1 General.** Software shall interoperate with assistive technology and shall conform to 502.
 - **EXCEPTION:** ICT conforming to 402 shall not be required to conform to 502.
- **502.2 Documented Accessibility Features.** Software with platform features defined in platform documentation as accessibility features shall conform to 502.2.
 - **502.2.1 User Control of Accessibility Features.** Platform software shall provide user control over platform features that are defined in the platform documentation as accessibility features.
 - **502.2.2 No Disruption of Accessibility Features.** Software shall not disrupt platform features that are defined in the platform documentation as accessibility features.
- **502.3 Accessibility Services.** Platform software and software tools that are provided by the platform developer shall provide a documented set of accessibility services that support applications running on the platform to interoperate with assistive technology and shall conform to 502.3. Applications that are also platforms shall expose the underlying platform accessibility services or implement other documented accessibility services.
 - **502.3.1 Object Information.** The object role, state(s), properties, boundary, name, and description shall be programmatically determinable.
 - **502.3.2 Modification of Object Information.** States and properties that can be set by the user shall be capable of being set programmatically, including through assistive technology.
 - **502.3.3 Row, Column, and Headers.** If an object is in a data table, the occupied rows and columns, and any headers associated with those rows or columns, shall be programmatically determinable.
 - **502.3.4 Values.** Any current value(s), and any set or range of allowable values associated with an object, shall be programmatically determinable.
 - **502.3.5 Modification of Values.** Values that can be set by the user shall be capable of being set programmatically, including through assistive technology.
 - **502.3.6 Label Relationships.** Any relationship that a component has as a label for another component, or of being labeled by another component, shall be programmatically determinable.
 - **502.3.7 Hierarchical Relationships.** Any hierarchical (parent-child) relationship that a component has as a container for, or being contained by, another component shall be programmatically determinable.

- **502.3.8 Text.** The content of text objects, text attributes, and the boundary of text rendered to the screen, shall be programmatically determinable.
- **502.3.9 Modification of Text.** Text that can be set by the user shall be capable of being set programmatically, including through assistive technology.
- **502.3.10 List of Actions.** A list of all actions that can be executed on an object shall be programmatically determinable.
- **502.3.11 Actions on Objects.** Applications shall allow assistive technology to programmatically execute available actions on objects.
- **502.3.12 Focus Cursor.** Applications shall expose information and mechanisms necessary to track focus, text insertion point, and selection attributes of user interface components.
- **502.3.13 Modification of Focus Cursor.** Focus, text insertion point, and selection attributes that can be set by the user shall be capable of being set programmatically, including through the use of assistive technology.
- **502.3.14 Event Notification.** Notification of events relevant to user interactions, including but not limited to, changes in the component's state(s), value, name, description, or boundary, shall be available to assistive technology.
- **502.4 Platform Accessibility Features.** Platforms and platform software shall conform to the requirements in ANSI/HFES 200.2, Human Factors Engineering of Software User Interfaces-Part 2: Accessibility (2008) (incorporated by reference, *see* 702.4.1) listed below:
 1. Section 9.3.3 Enable sequential entry of multiple (chorded) keystrokes;
 2. Section 9.3.4 Provide adjustment of delay before key acceptance;
 3. Section 9.3.5 Provide adjustment of same-key double-strike acceptance;
 4. Section 10.6.7 Allow users to choose visual alternative for audio output;
 5. Section 10.6.8 Synchronize audio equivalents for visual events;
 6. Section 10.6.9 Provide speech output services; and
 7. Section 10.7.1 Display any captions provided.

503 Applications

- **503.1 General.** Applications shall conform to 503.
- **503.2 User Preferences.** Applications shall permit user preferences from platform settings for color, contrast, font type, font size, and focus cursor.
 - **EXCEPTION:** Applications that are designed to be isolated from their underlying platform software, including Web applications, shall not be required to conform to 503.2.

- **503.3 *Alternative User Interfaces.*** Where an application provides an alternative user interface that functions as assistive technology, the application shall use platform and other industry standard accessibility services.
- **503.4 *User Controls for Captions and Audio Description.*** Where ICT displays video with synchronized audio, ICT shall provide user controls for closed captions and audio descriptions conforming to 503.4.
 - **503.4.1 *Caption Controls.*** Where user controls are provided for volume adjustment, ICT shall provide user controls for the selection of captions at the same menu level as the user controls for volume or program selection.
 - **503.4.2 *Audio Description Controls.*** Where user controls are provided for program selection, ICT shall provide user controls for the selection of audio descriptions at the same menu level as the user controls for volume or program selection.

504 Authoring Tools

- **504.1 *General.*** Where an application is an authoring tool, the application shall conform to 504 to the extent that information required for accessibility is supported by the destination format.
- **504.2 *Content Creation or Editing.*** Authoring tools shall provide a mode of operation to create or edit content that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.1 (incorporated by reference, *see* 702.10.1) for all supported features and, as applicable, to file formats supported by the authoring tool. Authoring tools shall permit authors the option of overriding information required for accessibility.
 - ***EXCEPTION:*** Authoring tools shall not be required to conform to 504.2 when used to directly edit plain text source code.
 - **504.2.1 *Preservation of Information Provided for Accessibility in Format Conversion.*** Authoring tools shall, when converting content from one format to another or saving content in multiple formats, preserve the information required for accessibility to the extent that the information is supported by the destination format.
 - **504.2.2 *PDF Export.*** Authoring tools capable of exporting PDF files that conform to ISO 32000-1:2008 (PDF 1.7) shall also be capable of exporting PDF files that conform to ANSI/AIIM/ISO 14289-1:2016 (PDF/UA-1) (incorporated by reference, *see* 702.3.1).
- **504.3 *Prompts.*** Authoring tools shall provide a mode of operation that prompts authors to create content that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.1 (incorporated by reference, *see* 702.10.1) for supported features and, as applicable, to file formats supported by the authoring tool.
- **504.4 *Templates.*** Where templates are provided, templates allowing content creation that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.1 (incorporated by reference, *see* 702.10.1) shall be provided for a range of template uses for supported features and, as applicable, to file formats supported by the authoring tool.

Chapter 6: Support Documentation and Services

601 General

- **601.1 Scope.** The technical requirements in Chapter 6 shall apply to ICT support documentation and services where required by Chapter 2 (Scoping Requirements) and where otherwise referenced in any other chapter of these Standards.

602 Support Documentation

- **602.1 General.** Documentation that supports the use of ICT shall conform to 602.
- **602.2 Accessibility and Compatibility Features.** Documentation shall list and explain how to use the accessibility and compatibility features required by Chapters 4 and 5. Documentation shall include accessibility features that are built-in and accessibility features that provide compatibility with assistive technology.
- **602.3 Electronic Support Documentation.** Documentation in electronic format, including Web-based self-service support, shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.1 (incorporated by reference, see 702.10.1).
- **602.4 Alternate Formats for Non-Electronic Support Documentation.** Where support documentation is only provided in non-electronic formats, alternate formats usable by individuals with disabilities shall be provided upon request.

603 Support Services

- **603.1 General.** ICT support services including, but not limited to, help desks, call centers, training services, and automated self-service technical support, shall conform to 603.
- **603.2 Information on Accessibility and Compatibility Features.** ICT support services shall include information on the accessibility and compatibility features required by 602.2.
- **603.3 Accommodation of Communication Needs.** Support services shall be provided directly to the user or through a referral to a point of contact. Such ICT support services shall accommodate the communication needs of individuals with disabilities.

Chapter 7: Referenced Standards

701 General

- **701.1 Scope.** The standards referenced in Chapter 7 shall apply to ICT where required by Chapter 2 (Scoping Requirements) and where referenced in any other chapter of these Standards.

702 Incorporation by Reference

- **702.1 Approved IBR Standards.** The following standards are incorporated by reference (IBR):
- **702.2 Advanced Television Systems Committee (ATSC).** Copies of the referenced standard may be obtained from the Advanced Television Systems Committee, 1776 K Street NW., Suite 200, Washington, DC 20006-2304 (<http://www.atsc.org>).
 - **702.2.1 ATSC A/53 Part 5:2014, Digital Television Standard, Part 5-AC-3 Audio System Characteristics,** August 28, 2014, IBR for 414.1.1.

- **702.3 Association for Information and Image Management (AIIM).** Copies of the referenced standard may be obtained from AIIM, 1100 Wayne Ave., Ste. 1100, Silver Spring, Maryland 20910 (http://www.aiim.org/Resources/Standards/AIIM_ISO_14289-1).
 - **702.3.1 ANSI/AIIM/ISO 14289-1-2016, Document Management Applications-Electronic Document File Format Enhancement for Accessibility-Part 1: Use of ISO 32000-1 (PDF/UA-1),** ANSI-approved February 8, 2016, IBR for 504.2.2.
- **702.4 Human Factors and Ergonomics Society (HFES).** Copies of the referenced standard may be obtained from the Human Factors and Ergonomics Society, P.O. Box 1369, Santa Monica, CA 90406-1369 (<http://www.hfes.org/Publications/ProductDetail.aspx?Id=76>).
 - **702.4.1 ANSI/HFES 200.2, Human Factors Engineering of Software User Interfaces-Part 2: Accessibility,** copyright 2008, IBR for 502.4.
- **702.5 Institute of Electrical and Electronics Engineers (IEEE).** Copies of the referenced standard may be obtained from the Institute of Electrical and Electronics Engineers, 10662 Los Vaqueros Circle, P.O. Box 3014, Los Alamitos, CA 90720-1264 (<http://www.ieee.org>).
 - **702.5.1 ANSI/IEEE C63.19-2011, American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids,** May 27, 2011, IBR for 412.3.1.
- **702.6 International Code Council (ICC).** Copies of the referenced standard may be obtained from ICC Publications, 4051 W. Flossmoor Road, Country Club Hills, IL 60478-5795 (<http://www.iccsafe.org>).
 - **702.6.1 ICC A117.1-2009, Accessible and Usable Buildings and Facilities,** approved October 20, 2010, IBR for 402.5.
- **702.7 International Telecommunications Union Telecommunications Standardization Sector (ITU-T).** Copies of the referenced standards may be obtained from the International Telecommunication Union, Telecommunications Standardization Sector, Place des Nations CH-1211, Geneva 20, Switzerland (<http://www.itu.int/en/ITU-T>).
 - **702.7.1 ITU-T Recommendation E.161, Series E. Overall Network Operation, Telephone Service, Service Operation and Human Factors-International operation-Numbering plan of the international telephone service, Arrangement of digits, letters and symbols on telephones and other devices that can be used for gaining access to a telephone network,** February 2001, IBR for 407.3.3.
 - **702.7.2 ITU-T Recommendation G.722.2, Series G. Transmission Systems and Media, Digital Systems and Networks-Digital terminal equipment-Coding of analogue signals by methods other than PCM, Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB),** July 2003, IBR for 412.4.
- **702.8 Internet Engineering Task Force (IETF).** Copies of the referenced standard may be obtained from the Internet Engineering Task Force (<http://www.ietf.org>).

- **702.8.1 IETF RFC 6716, Definition of the Opus Codec**, September 2012, J.M. Valin, Mozilla Corporation, K. Vos, Skype Technologies S.A., T. Terriberry, Mozilla Corporation, IBR for 412.4.
- **702.9 Telecommunications Industry Association (TIA)**. Copies of the referenced standard, published by the Telecommunications Industry Association, may be obtained from IHS Markit, 15 Inverness Way East, Englewood, CO 80112 (<http://global.ihs.com>).
 - **702.9.1 TIA-1083-B, Telecommunications-Communications Products-Handset Magnetic Measurement Procedures and Performance Requirements**, October 2015, IBR for 412.3.2.
- **702.10 Worldwide Web Consortium (W3C)**. Copies of the referenced standard may be obtained from the W3C Web Accessibility Initiative, Massachusetts Institute of Technology, 32 Vassar Street, Room 32-G515, Cambridge, MA 02139 (<http://www.w3.org/TR/WCAG21>).
 - **702.10.1 WCAG 2.1, Web Content Accessibility Guidelines**, W3C Recommendation, September 21, 2023, IBR for: E205.4, E205.4 Exception, E205.4.1, E207.2, E207.2 Exception 2, E207.2 Exception 3, E207.2.1, E207.3, 408.3 Exception, 501.1 Exception, 504.2, 504.3, 504.4, and 602.3.

Contract # LS5021

STATE OF UTAH COOPERATIVE CONTRACT

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

<u>SHI International Corp</u>		
Name		
<u>290 Davidson Ave</u>		
Address		
<u>Somerset</u>	<u>NJ</u>	<u>08873</u>
City	State	Zip

LEGAL STATUS OF CONTRACTOR

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

Contact Person Katelyn Rispoli Phone #1-732-584-8425 Email Katelyn_Rispoli@SHI.com
 Vendor #33386DD 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
 ATTACHMENT H: SHI Return Policy
Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.
7. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this Contract.
 - Utah State Procurement Code, Procurement Rules, the Solicitation, and Contractor's response to the Solicitation. Both the solicitation and Contractor's response to the solicitation, while not included as a listed attachment to the Master Agreement above, will both be available on the NASPO website for transparency less any information marked as confidential by the Contractor at the time of submission
8. Each person signing this Contract represents and warrants that he/she is duly authorized and has legal capacity to execute and deliver this Contract and bind the parties hereto. Each signatory represents and warrants to the other that the execution and delivery of the Contract and the performance of each party's obligations hereunder have been duly authorized and that the Contract is a valid and legal Contract binding on the parties and enforceable in accordance with its terms.
 IN WITNESS WHEREOF, the parties sign and cause this Contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 4 above.

CONTRACTOR

Signed by:

Kristina Mann
 Contractor's Signature

Kristina Mann

Print Name

Director - Contract

Title

Date

2/26/2026

STATE

Signed by:

Rick Straw
 Director, Division of Purchasing

2/26/2026

Date

ATTACHMENT A

NASPO VALUEPOINT MASTER AGREEMENT TERMS AND CONDITIONS

Negotiated 12.1 and 12.3.

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. Additionally, Data
- 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 Contract and/or receive a Product, including an End User License Agreement (EULA), customer agreement, memorandum of understanding, Statement of Work, lease agreement, Service Level Agreement (SLA), 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 a Master Agreement or 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, 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 (SLA)** means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) the amount of time required for notice by the provider to the public jurisdiction of upcoming changes, (3) security notice requirements, (4) timeframes for response to operational problems and failures, (5) description of service quality, (6) identification of roles and responsibilities, (7) remedies,

such as credits, and (8) an explanation of how remedies or credits are calculated and issued.

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

1.30 Solicitation means the Solicitation resulting in this Master Agreement.

II. Term of Master Agreement

- 2.1 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.
- 2.2 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.
- 2.3 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

- 3.1 Order.** Any Order placed under this Master Agreement will consist of the following documents:
 - 3.1.1** A Participating Entity's Participating Addendum ("PA");
 - 3.1.2** Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions, including all attachments thereto;
 - 3.1.3** A Purchase Order or Scope of Work/Specifications issued against the Master Agreement;
 - 3.1.4** The Solicitation or, if separately executed after award, the Lead State's bilateral agreement that integrates applicable provisions;
 - 3.1.5** Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State.
 - 3.1.6** 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.

- 3.2 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.
- 3.3 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

- 4.1 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.
- 4.2 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.
- 4.3 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.
- 4.4 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.
- 4.5 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.
- 4.6 Participating Entities.**

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

5.1 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.

5.2 Administrative Fees

5.2.1 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.

5.2.2 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.

5.3 NASPO ValuePoint Summary and Detailed Usage Reports

5.3.1 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.

- 5.3.2 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.
- 5.3.3 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.
- 5.3.4 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.
- 5.3.5 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.
- 5.3.6 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.

5.4 NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review

- 5.4.1 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.
- 5.4.2 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.
- 5.4.3 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.
- 5.4.4 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.
- 5.4.5 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.

5.5 NASPO ValuePoint eMarketPlace

- 5.5.1** 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.

- 5.5.2** 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.
- 5.5.3** 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.
- 5.5.4** 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.
- 5.5.5** 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.
- 5.5.6** Contractor's use of the eMarketPlace shall comply with the eMarketPlace's Terms of Use.
- 5.5.7** 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.
- 5.5.8** 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.
- 5.5.9** 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.

5.5.10 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.

5.5.11 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.

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

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

5.5.11.3 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.

5.5.11.3.1 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.

5.5.11.3.2 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.

5.5.11.3.3 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.

5.5.12 Hosted catalogs and punchout sites will provide all of the eMarketPlace standard Data elements/information including, but not limited to, the

following:

- 5.5.12.1** 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;
- 5.5.12.2** A Lead State contract identification number for this Master Agreement;
- 5.5.12.3** Detailed Product line item descriptions;
- 5.5.12.4** Pictures illustrating Products, services, or solutions where practicable; and
- 5.5.12.5** Any additional NASPO, Lead State, or Participating Addendum requirements.

5.6 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.

5.7 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.

5.8 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

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

6.1.1 All rates and discounts must be guaranteed for the initial term of the Master Agreement.

6.1.2 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.

6.1.3 No retroactive adjustments to prices or rates will be allowed.

6.2 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.

6.3 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

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

7.2 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.

7.3 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.

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

7.5 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.

- 7.5.1 Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or performance period up to 120 days past the then-current termination date of this Master Agreement.
 - 7.5.2 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.
 - 7.5.3 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.
 - 7.5.4 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.
 - 7.5.5 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.
 - 7.5.6 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.
- 7.6 **Order Form Requirements.** All Orders pursuant to this Master Agreement, at a minimum, must include:
 - 7.6.1 The services or supplies being delivered;
 - 7.6.2 A shipping address and other delivery requirements, if any;
 - 7.6.3 A billing address;
 - 7.6.4 Purchasing Entity contact information;
 - 7.6.5 Pricing consistent with this Master Agreement and applicable Participating Addendum and as may be adjusted by agreement of the Purchasing Entity and Contractor;
 - 7.6.6 A not-to-exceed total for the Products or Services being ordered; and
 - 7.6.7 The Master Agreement number or the applicable Participating Addendum number, provided the Participating Addendum references the Master Agreement number.
- 7.7 **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.

- 7.8 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

- 8.1 Shipping Terms.** All deliveries will be F.O.B. destination, freight pre-paid, with all transportation and handling charges paid by the Contractor.
- 8.1.1** 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.
- 8.2 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.
- 8.3 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.
- 8.4 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

- 9.1 Laws and Regulations.** Any and all Products offered and furnished must comply fully with all applicable Federal, State, and local laws and regulations.
- 9.2 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.
- 9.3 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.

9.3.1 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.

9.3.2 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.

9.4 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.

9.5 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.

9.5.1 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.

9.5.2 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.

9.5.3 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.

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

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

X. Warranty

10.1 Applicability. Unless otherwise specified in the Master Agreement, Participating

Addendum, or ordering document, the terms of this Section X will apply.

- 10.2 Warranty.** The Contractor warrants for a period of one year 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.
- 10.3 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.
- 10.4 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.
- 10.5 Warranty Period Start Date.** The warranty period will begin upon Acceptance, as set forth in Section IX.

XI. Product Title

- 11.1 Conveyance of Title.** 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.
- 11.2 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.
- 11.3 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

- 12.1 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 directly from any negligent or willful act, error, or omission of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to performance under this Master Agreement

12.2 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").

- 12.2.1** 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:
 - 12.2.1.1** provided by the Contractor or the Contractor's subsidiaries or affiliates;
 - 12.2.1.2** specified by the Contractor to work with the Product;
 - 12.2.1.3** 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
 - 12.2.1.4** reasonably expected to be used in combination with the Product.
- 12.2.2** 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.
- 12.2.3** 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.
- 12.2.4** 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.

12.3 Limitation of Liability

Limitation of Liability: Except for (a) claims, losses, and liabilities arising from a Party’s gross negligence or willful misconduct; (b) claims, losses, and liabilities arising from death, injury, or damage to tangible property; (c) claims, losses, and liabilities arising from a Party’s violation of applicable law; and (d) each Party’s indemnification obligations, each Party’s aggregate liability to the other Party for all other claims (including for direct damages) under this Master Agreement, a Participating Addendum, or an Order, shall not exceed the greater of (i) five million dollars (\$5,000,000), or (ii) the total fees paid and payable in the twenty-four (24) months immediately preceding the event giving rise to liability.

Contractor shall not be liable for incidental, punitive, or indirect damages.

XIII. Insurance

- 13.1 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.
- 13.2 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.
- 13.3 Coverage. Coverage must be written on an occurrence basis. The minimum acceptable limits will be as indicated below:

13.3.1 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;

13.3.2 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

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

- 13.4 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.

- 13.5 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.
- 13.6 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.
- 13.7 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.
- 13.8 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

14.1 Records Administration and Audit

- 14.1.1** 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.
- 14.1.2** 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.

- 14.1.3** 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.

14.2 Confidentiality, Non-Disclosure, and Injunctive Relief

- 14.2.1 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.

- 14.2.1.1** 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").

- 14.2.1.2** 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.

- 14.2.1.3** 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.

- 14.2.2 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.

- 14.2.2.1** 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.
- 14.2.2.2** 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.
- 14.2.2.3** 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.
- 14.2.2.4** 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.
- 14.2.3** **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.
- 14.2.4** **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.
- 14.2.5** **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.

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

14.2.7 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.

14.2.7.1 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.

14.3 Assignment/Subcontracts

14.3.1 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.

14.3.2 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.

14.4 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.

14.5 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.

14.6 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.

14.7 Force Majeure. Neither party to this Master Agreement shall be held responsible for delay or default caused by fire, riot, unusually severe weather, other acts of God, or acts of war which are beyond that party's reasonable control. The Lead State may terminate this Master Agreement upon determining such delay or default will reasonably prevent successful performance of the Master Agreement.

14.8 Defaults and Remedies

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

14.8.1.1 Nonperformance of contractual requirements;

14.8.1.2 A material breach of any term or condition of this Master Agreement;

14.8.1.3 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;

14.8.1.4 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

14.8.1.5 Any default specified in another section of this Master Agreement.

14.8.2 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.

14.8.3 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:

14.8.3.1 Any remedy provided by law;

14.8.3.2 Termination of this Master Agreement and any related Contracts or portions thereof;

14.8.3.3 Assessment of liquidated damages as provided in this Master Agreement;

14.8.3.4 Suspension of Contractor from being able to respond to future bid solicitations;

14.8.3.5 Suspension of Contractor's performance; and

14.8.3.6 Withholding of payment until the default is remedied.

14.8.4 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.

14.9 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.

14.10 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.

14.11 No Waiver of Sovereign Immunity

14.11.1 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.

14.11.2 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.

14.12 Governing Law and Venue

14.12.1 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.

14.12.2 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.

14.12.3 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.

14.13 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.

14.14 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.
- 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 written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

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 (current version) 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 (current version). 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 (current version) 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 (current version) 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 (current version). 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. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

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 (current version) Access Controls.
- b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract.

- 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 the obligations of the contract who have been convicted of any crime of dishonesty. 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.

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.

- i. **Statement of Work:** A written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

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 (current version) 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 (current version). 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 (current version) 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 (current version) 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 (current version). 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. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

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 (current version) Access Controls.

Preventing any offshore access by service provider, employees and contractors, unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract.

- 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 the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or

otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to one year is an authorized penalty. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.

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.
- i. **Statement of Work:** A written statement in a solicitation document or contract that describes the public jurisdiction's service needs and expectations.

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 (current version) 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 (current version). 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 (current version) 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 (current version) 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 (current version). 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. The service provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this contract.

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 (current version) Access Controls.

- b. Preventing offshore access by service provider employees and contractors unless explicitly authorized by the public jurisdiction for Follow the Sun technical support under the contract.
- 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 the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud or any felony or misdemeanor offense with an authorized penalty of incarceration for up to one year. The service provider shall promote and maintain an awareness among its employees and agents of the importance of securing the public jurisdiction's information.

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. Value-Added Reseller: SAAS
2. Value-Added Reseller: IaaS
3. Value-Added Reseller: PaaS
4. Value-Added Reseller: On-Premise
5. Value-Added Reseller: Value Added Services

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

Definitions:

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

1. Definitions, Roles, and Responsibilities:

Direct Service Providers: A Direct Service Provider is the entity responsible for making a service available to Purchasing Entities. A Direct Service Provider for a cloud solution or other software solution could include an original equipment manufacturer ("OEM"), software publisher, etc. A Direct Service Provider for purposes of the Master Agreement is an entity who creates and has its own solutions, and provides their own cloud or software solutions or services, and typically sets the pricing for its own Products and Services that it provides. A Direct Service Provider may or may not necessarily sell directly

to customers and Purchasing Entities (it may onboard and utilize Fulfillment Partners and sell through the Fulfillment Partners exclusively as its authorized resellers as an example). A Direct Service Provider for an On-Premises solution would develop, maintain and support software that is installed locally on a consumer's system, hardware, or infrastructure and which is provided as Product under the Master Agreement.

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

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

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

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

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

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

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

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

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

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

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

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

2. Categorization of Risk

Contractor must store and secure one, all, or a combination of data¹ Risk categories of the data are defined as:

a. Low Risk Data

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

Low Impact levels are defined in FIPS 199 as follows:

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

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

b. Moderate Risk Data

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

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

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

c. High Risk Data

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

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

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

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

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

3. Service Models

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

Award Categories:

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

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

1. **Software as a Service (SaaS)** - as used in this Master Agreement is defined as the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Full terms and conditions applicable to SaaS are located in Attachment A NASPO Master Agreement Terms and Conditions.
2. **Infrastructure as a Service (IaaS)** - as used in this Master Agreement is defined as the capability provided to the consumer for provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls). Full terms and conditions applicable to IaaS are located in Attachment A NASPO Master Agreement Terms and Conditions.
3. **Platform as a Service (PaaS)** - as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Full terms and conditions applicable to PaaS are located in Attachment A NASPO Master Agreement Terms and Conditions.
4. **On-Premises** – as used in this Master Agreement is defined as Products and Services installed or provided locally on a consumer's hardware, servers, or other infrastructure. On-Premises solutions are not cloud solutions. Consumer maintains and has control over their operating systems, hardware, and infrastructure. Appropriate terms and conditions applicable to On-Premises solutions are being deferred to Participating Entities to negotiate in its Participating Addendum (PA). As On-Premises solutions are unique to each entity and involve individual jurisdictions and applicable code, rule, regulations, and statutes that will oversee this Service Model. This allows each Participating Entity to place its own mandatory requirements.

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

4. Deployment Models

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

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

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

II. NEW TECHNOLOGY

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

III. CATALOG UPDATES

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

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

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

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

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

Attachment C Pricing Discounts and Schedule

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

Minimum Discount % Off MSRP	Software (Saas)	Infrastructure (Iaas)	Platform (Paas)	On-Premises	Value Added Services*
Value-Added Resellers: Minimum Discount % off MRSP * (also applies to all Third-party solutions or services offered within this Value Added Services category)	1.50%	1.50%	1.50%	1.50%	1%
Maximum Markup %	Software (Saas)	Infrastructure (Iaas)	Platform (Paas)	On-Premises	Value Added Services*
Value-Added Resellers: Maximum Markup %	20%	20%	20%	20%	30%

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.

