Contract #: AR3105

STATE OF UTAH COOPERATIVE CONTRACT

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

Human Resources Technologies, Incorporated
Name

5400 Shawnee Road, Suite 201
Street Address

Alexandria	VA	22312
City	*State*	*Zip*

Vendor # VC226572 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact *Name:* Douglas L Sears *Phone Number:* 703-719-0078 *Email:* dsears@hrtec.net

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Friday, March 15, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative 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) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs, etc.

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

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

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 5 above.

CONTRACTOR

Douglas L. Sears — Mar 13, 2019

Contractor's signature — Date

Douglas Sears — Executive Director

Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes — Mar 13, 2019

Christopher Hughes (Mar 13, 2019)

Director, Division of Purchasing — Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall 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.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means 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.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

Data means all information, whether in oral or written (including electronic) form,

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

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.

Data Breach means any actual or reasonably suspected non-authorized 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 the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined 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).

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.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

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

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

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

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the 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 and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

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.

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

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate.

Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

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.

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.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

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.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing

Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

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) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (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.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. 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's or Purchasing Entity's clients. 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. 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.

b. 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. 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. 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. 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. 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.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in 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.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint'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. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(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; or

(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

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 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 shall not diminish or eliminate Contractor's liability for damages.

c. 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 Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. 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 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. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to 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.

12. Force Majeure: Neither party shall be in default by reason of any failure in

performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("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 ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order 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

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(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 and then only to the extent of the prejudice or expenses. If the Contractor promptly and

reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. 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 it 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. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have 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 agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

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

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. 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 Best's 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.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability 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/$3 million general

aggregate;

(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

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. 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) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states);

a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a 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.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating 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.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms 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 Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. 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.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall 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.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that 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.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to 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 or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, 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.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The 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. By way 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.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. 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. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right 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.

26. Records Administration and Audit.

a. 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 shall 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 shall 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 Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. 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.

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

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The 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 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. 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 shall 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, Participating Addendum, or Purchase Order.

34. 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 to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) 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.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall 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 shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. 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 Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall 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 shall be in the Purchasing Entity's State.

c. 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; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating 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.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. 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.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data

within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to 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 qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements 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.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

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 a 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. This obligation shall survive and extend beyond the term of this Master Agreement.

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

a. The Contractor 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 recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

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

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor 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 Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity 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 Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

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

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity 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 as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, 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 in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor 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 responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, 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 Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

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 a 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. This obligation shall survive and extend beyond the term of this Master Agreement.

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

a. The Contractor 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 recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

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

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Incident Response: The Contractor 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 Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity 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 Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity 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 as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, 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 in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor 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 responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, 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 Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

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 a 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. This obligation shall survive and extend beyond the term of this Master Agreement.

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

a. The Contractor 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 recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

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

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

b. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity 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 Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity 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 as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted

and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, 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 in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor 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 responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, 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 Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. **Subscription Terms:** Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
IaaS	X	X	X	Private, Community, Hybrid
PaaS	X	X	X	Private, Community, Hybrid
SaaS	X	X	X	Private, Community, Hybrid

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **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.
- **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.
- **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.
- **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)

Attachment C - Pricing Discounts and Schedule

Contractor Human Resoruces Technologies, Inc.

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.

2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.

4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Infrastructure as a Service (IaaS)	
Description	Minimum Discount % Off
IaaS Minimum Discount % * (applies to all OEM's offered within this IaaS model)	20.00%
Average IaaS OEM Discount Off	**20.00%**

Cloud Service Model: Platform as a Service (PaaS)	
Description	Discount
PaaS Minimum Discount % * (applies to all OEM's offered within this PaaS model)	20.00%
Average PaaS OEM Discount Off	**20.00%**

Cloud Service Model: Software as a Service (SaaS)	
Description	Discount
SaaS Minimum Discount % * (applies to all OEM's offered within this SaaS model	20.00%
Average SaaS OEM Discount Off	**20.00%**

Additional Value Added Services

	Onsite Hourly Rate		Remote Hourly Rate	
Item Description	**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Sr. Application Specialist	$ 144.14	$ 165.68	$ 152.43	$ 165.68
Application Specialist	$ 104.23	$ 119.81	$ 110.23	$ 119.81
Jr. Application Specialist	$ 53.06	$ 60.99	$ 56.11	$ 60.99
Sr. Principal Engineer	$ 177.74	$ 204.30	$ 187.96	$ 204.30
Principal Engineer	$ 144.05	$ 165.58	$ 152.33	$ 165.58
Sr. Programmer/Web Application Developer	$ 146.37	$ 168.24	$ 154.78	$ 168.24
Programmer/Web Application Developer	$ 98.75	$ 113.50	$ 104.42	$ 113.50
Jr. Programmer/Web Application Developer	$ 55.24	$ 63.49	$ 58.41	$ 63.49
Sr. Web Developer	$ 145.60	$ 167.36	$ 153.97	$ 167.36
Web Developer	$ 87.37	$ 100.43	$ 92.40	$ 100.43
Jr. Web Developer	$ 51.83	$ 59.57	$ 54.80	$ 59.57
Program Manager	$ 198.41	$ 228.06	$ 209.82	$ 228.06
Project Manager	$ 171.95	$ 197.64	$ 181.83	$ 197.64
Sr. Technical Task Manager	$ 128.18	$ 147.33	$ 135.54	$ 147.33
Technical Task Manager	$ 104.51	$ 120.13	$ 110.52	$ 120.13
Sr. Program Control Specialist	$ 55.12	$ 63.36	$ 58.29	$ 63.36
Program Control Specialist	$ 31.33	$ 36.01	$ 33.13	$ 36.01
Sr. Network Administrator	$ 131.15	$ 150.75	$ 138.69	$ 150.75
Network Administrator	$ 100.67	$ 115.71	$ 106.45	$ 115.71
Jr. Network Administrator	$ 49.60	$ 57.01	$ 52.45	$ 57.01
Sr. Network Engineer	$ 144.14	$ 165.68	$ 152.43	$ 165.68
Network Engineer	$ 104.23	$ 119.81	$ 110.23	$ 119.81
Jr. Network Engineer	$ 55.33	$ 63.60	$ 58.51	$ 63.60
Sr. Database Administrator	$ 119.40	$ 137.24	$ 126.26	$ 137.24
Database Administrator	$ 90.12	$ 103.59	$ 95.30	$ 103.59
Jr. Database Administrator	$ 53.06	$ 60.99	$ 56.11	$ 60.99

Attachment C - Pricing Discounts and Schedule

Contractor Human Resoruces Technologies, Inc.

Principal Security Engineer/Analyst	$ 282.55	$ 324.77	$ 298.79	$ 324.77
Sr. Security Engineer/Analyst	$ 241.80	$ 277.93	$ 255.70	$ 277.93
Security Engineer/Analyst	$ 208.20	$ 239.31	$ 220.17	$ 239.31
Associate Security Engineer/Analyst	$ 178.00	$ 204.60	$ 188.23	$ 204.60
Sr. Business/Systems Analyst	$ 144.14	$ 165.68	$ 152.43	$ 165.68
Business/Systems Analyst	$ 104.23	$ 119.81	$ 110.23	$ 119.81
Jr. Business/Systems Analyst	$ 72.11	$ 82.88	$ 76.25	$ 82.88
Sr. Training Instructor	$ 104.88	$ 120.55	$ 110.91	$ 120.55
Training Instructor	$ 87.26	$ 100.30	$ 92.28	$ 100.30
Sr. Data Technician	$ 81.21	$ 93.35	$ 85.88	$ 93.35
Data Technician	$ 47.33	$ 54.40	$ 50.05	$ 54.40
Help Desk Specialist	$ 81.21	$ 93.35	$ 85.88	$ 93.35
Help Desk Technician	$ 61.67	$ 70.89	$ 65.22	$ 70.89
Sr. Technical Writer/Documentation Specialist	$ 101.73	$ 116.93	$ 107.58	$ 116.93
Technical Writer	$ 89.02	$ 102.32	$ 94.13	$ 102.32
Sr. Graphic Specialist	$ 90.12	$ 103.59	$ 95.30	$ 103.59
Graphic Specialist	$ 57.30	$ 65.86	$ 60.59	$ 65.86
Technical Support (H/W, S/W set-up)	$ 100.53	$ 115.55	$ 106.31	$ 115.55

DOCUMENT 6: TECHNICAL RESPONSE

This document should constitute the Offeror's response to the items described in Section 8 of the RFP, and must contain at least the following information:

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

A. For over 30 years HRTec has served the Armed Forces Community, Federal Agencies, Non-Profits, and private industry with secure worldwide human resources telecommunications networks and hosted services. We have continuously maintained an unusually robust, flexible intranet services capability that provides fast, reliable access and connectivity from any location around the world. Since 2010, HRTec cloud service offerings and solutions have been purpose built to provide comprehensive technical and security support to our customers. We consistently receive accolades for providing high quality support for the customer systems and services managed / hosted within our secure full-service stack of cloud offerings.

Upon award of the NASPO ValuePoint Cloud Solution Master Service Agreement HRTec will establish a State and Local Government, and Education (SLED) community enclave within our **Federal High Impact Virtualized Environment (FedHIVE)** cloud services datacenters located in Alexandria, VA and Bedford, NH. Our Cloud Services Offerings as defined in this proposal leverage the design, infrastructure and high-level baseline security controls established in our existing FedHIVE IaaS/PaaS.

Always mindful of the importance of protecting our customers data, we have a long history of implementing DoD and other agency security policies and controls within our datacenters and our applications, from DoD Information Assurance Certification and Accreditation Process (DIACAP) to Federal Information Security Management Act (FISMA) then the National Institute of Standards and Technology Risk Management Framework (NIST RMF) and currently the Federal Risk and Authorization Management Program (FedRAMP) and the Cloud Security Alliance (CSA) Security Trust & Assurance Registry (STAR).

FedHIVE is a FedRAMP Ready High Impact Virtualized Environment (IaaS/PaaS) and is where we host our secure SaaS suite of customizable solutions that are purpose-built for defense, federal civilian, and other governmental agency and educational institute requirements.

The CSA STAR program provides the most comprehensive set of Confidentiality, Integrity, and Availability controls specific to the Cloud. The most powerful program for security assurance in the Cloud Industry encompassing key principles of transparency, rigorous auditing, and harmonization of standards, including indications of best practices and validation of security postures of cloud offerings.

In 2017, HRTec launched FedHIVE as a FedRAMP High Impact Baseline and DoD Cloud Computing Security Requirements Guide – Impact Level 4 security control compliant Cloud Service Offering (CSO). FedHIVE is complaint with for Infrastructure-as-a-Service (IaaS) and Platform as a Service (PaaS) that is

compliant with FedRAMP High Impact Baseline security controls and includes additional controls and control enhancements beyond the 421 required NIST SP 800-53r4 high impact security controls.

DOD Impact Level 4 security controls are designed to accommodate DoD Controlled Unclassified Information (CUI) and/or other mission critical data to include that used in direct support of military or contingency operations. CUI is information the Federal Government creates or possesses that a law, regulation, or Government-wide policy requires, or specifically permits, an agency to handle by means of safeguarding or dissemination controls.

Commercial DoD Impact Level 4 CSP/CSO customers may include all US government customers (Federal, State, Local, and Tribal) and commercial customers which support them. In some cases, a Level 4 Provisional Authorization (PA) may be granted to CSOs that support other commercial entities, but not the general public. HRTec is currently in the queue and actively engaging with the FedRAMP PMO to obtain prioritization to obtain a FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the High Impact Baseline. The JAB P-ATO process supports a concurrent review for the DoD Level 4 PA. This is significant as only four other offerings have received this level of authorization for IaaS and PaaS. FedHIVE is likely to be the first non-leveraged Small Business provisioned commercial private, community, and/or Hybrid CSO. The FedHIVE Secure CSO provides agencies with a customer service focused, agile, and highly secure offering to support any agency need.

For the NASPO ValuePoint MSA, in addition to FedHIVE IaaS and PaaS HRTec is proposing two Software as a Service (SaaS) offerings from our Discern Secure SaaS Suite that are provisioned exclusively within our FedHIVE IaaS/PaaS where we can ensure those products meet and exceed all industry service and information security best practices as well as all meet or exceed all government regulatory and compliance requirements for secure CSOs.

Discern EO Manager (SaaS)

HRTec's Discern EEO Manager is a proven EEO case management SaaS product that has been in use for over 15 years by DoD service components and other federal agencies to remain current with Equal Employment Opportunity Commission (EEOC) annual reporting requirements (EEOC 462 and No Fear Reporting) and automate workflow and report generation.

HRTec developed this easy-to-use Equal Employment Opportunity (EEO) case management system application for this complex process. First deployed in 2001 at military installations throughout the US and overseas as MEONet for military servicemembers and later as EEONet for civilians this system has supported over 2500 user accounts across the DoD and a growing number of Federal Agencies.

EEO Manager was built to assist EEO managers and counselors throughout an organization manage all aspects of information and program management related to tracking EEO complaints and resolutions. Built to support the Equal Employment Opportunity Commission (EEOC) annual reporting requirements, EEONet allows automated generation of the reports required by EEOC as well as a variety of other reports and documentation that can be customized to user and management requirements. EEO Manager is Section 508 compliant.

The EEO Manager solution extends EEO program management capabilities and data access real-time via a secure, web-based system. It includes superior business logic and data entry flow, while offering the instant accessibility of a central database for the entire organization.

This SaaS offering is in use by the United States Military Entrance Processing Command, National Reconnaissance Office, U. S. Government Printing Office, National Transportation Safety Bureau, and Broadcasting Board of Governors.

Discern SCA&R Manager (SaaS)

SCA&R Manager is a HRTec developed and deployed survey and assessment system focused on assisting organizations with determining the effectiveness of organizational systems. This SaaS application collects data that is analyzed and assessed to produce actionable reports focused on customer/agency organizational climate. The system focuses on 13 human factors covering organizational effectiveness, equal opportunity, and job satisfaction.

Initially built for the specific purpose of collecting and reporting on organizational climate, SCA&R Manager has evolved to allow for other customization for secure survey-based assessment requirements including sensitive or protected data (e.g. safety surveys, customer feedback, patient healthcare data collection, etc.).

This document should constitute the Offeror's response to the items described in Section 8 of the RFP, and must contain at least the following information:

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

B. The remainder of this technical response is designed to provide a point-by point response to each requirement identified in Section 8 of the RFP.

6.1. Technical Requirements (RFP Section 8.1)

8.1.1. - For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

HRTec has purpose-built all cloud service offerings to meet government customer cloud needs and compliance requirements. Therefore, the NASPO ValuePoint customer base will benefit directly from our intentional focus on the NIST Risk Management Framework within a FedRAMP compliant high-impact baseline infrastructure. The proposed FedHIVE IaaS/PaaS and Discern SaaS Suite CSOs provide for all the NIST 800-145 defined essential characteristics as permitted by the implemented high impact security controls and supporting processes and procedures as follows:

- *On-demand self-service.* A customer/agency can provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction to extend current service products within the FedHIVE boundary. Due to the security posture of FedHIVE any provisioning of new capabilities or applications that have not been previously tested in the

HRTec Test and Development Environment (TDE) will require provisioning support from our Information Security Workforce (ISWF) to support testing within the TDE and transfer to the production environment.

- *Broad network access.* All HRTec CSO capabilities are available over the network and accessed through web-browsers promoting use by heterogeneous thin or thick client platforms (e.g., tablets, laptops, and workstations).
- *Resource pooling.* The FedHIVE infrastructure has been designed with multiple enclaves within the FedHIVE boundary that provided for community-based computing resources that are pooled to serve multiple community consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Currently we have two community enclaves Defense and Government. As previously stated, HRTec will establish a State and Local Government, and Education (SLED) community enclave within the FedHIVE cloud services datacenters located in Alexandria, VA and Bedford, NH upon award of the NASPO ValuePoint Cloud Solution Master Service Agreement. This SLED Enclave will provide for community-based resource pooling of storage, processing, memory, and network bandwidth for all SLED customers/agencies.
- *Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service.* The FedHIVE management enclave includes various tools that provide for automatic control and optimization of resource usage via inherent metering capabilities appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

8.1.2 - As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of **Attachments C & D**.

HRTec will demonstrate throughout our proposal and this technical response that we understand and will comply with the requirements identified in Attachment C: NIST Service Models and Attachment D: Scope of Services. HRTec affirms our ability and willingness to provide an isolated and secure stack of service models, service model subcategories, data risk categories and deployment models under the terms of the NVP Master Agreement for Cloud Solutions per the requirements of Attachments C and D. **Exhibit 6A: HRTec Cloud Service Models** illustrates the cloud services models HRTec proposes to serve the NASPO ValuePoint community. Our service models, including our SaaS offerings, leverage the design, infrastructure and high-level baseline security controls established in our FedHIVE IaaS/PaaS offering.

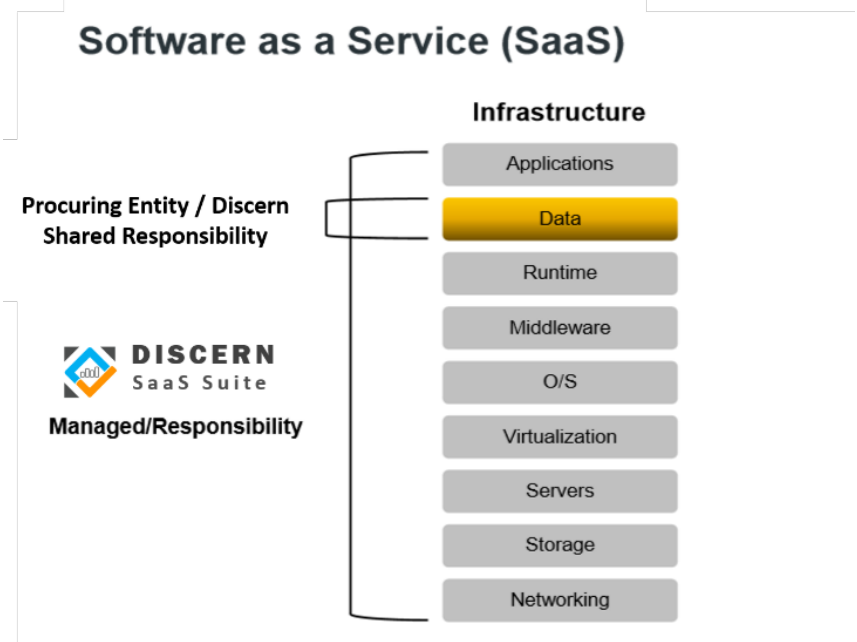
Exhibit 6A: HRTec Cloud Service Models

Service Model	Service Model Subcategory	Data Risk Category	Deployment Model
IaaS	Computer/Infrastructure Services, Disaster Recovery, Storage, Network, Security	Low, Moderate, & High	Private, Community, Hybrid
PaaS	Analytics, Database, Development, Testing and Deployment, Integration, Open Source	Low, Moderate, & High	Private, Community, Hybrid
SaaS	Analytics, Data Management, Electronic Records Management, Workflow, Case Management	Moderate, High	Private, Community, Hybrid

8.1.3 - As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in **Attachment D**.

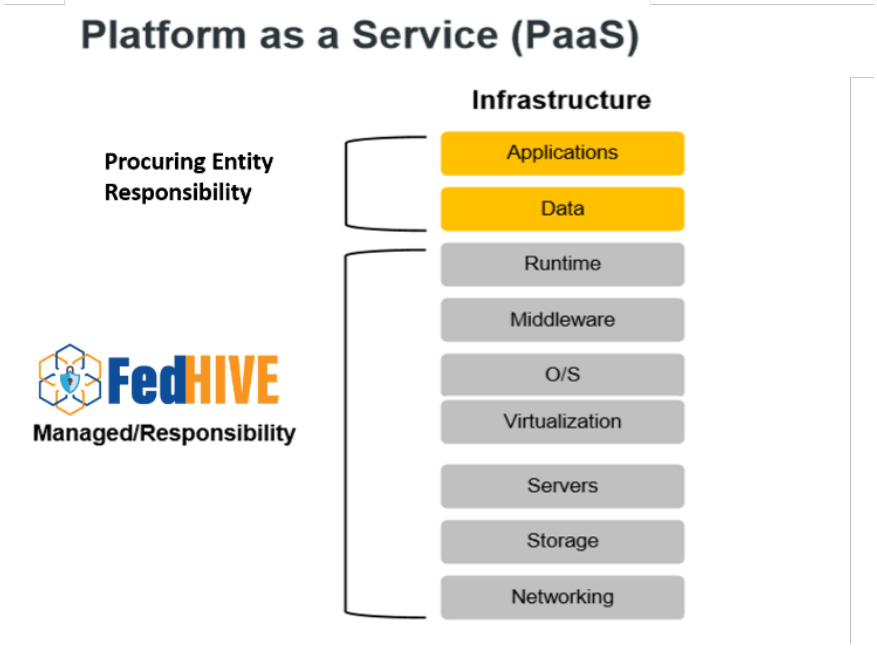
Software as a Service (SaaS) – The Discern SaaS Suite Offerings proposed for the NASPO MSA (EEO Manager and SCA&R Manager) are SaaS applications that are provisioned for customers/agencies within HRTec's FedHIVE cloud infrastructure. These SaaS applications are accessible by authorized users from customer approved devices via web-browser interface. **Exhibit 6B: HRTec Discern SaaS Suite Infrastructure** illustrates the division of management and control responsibilities of HRTec and the customer/agency.

Exhibit 6B: HRTec Discern SaaS Suite Infrastructure



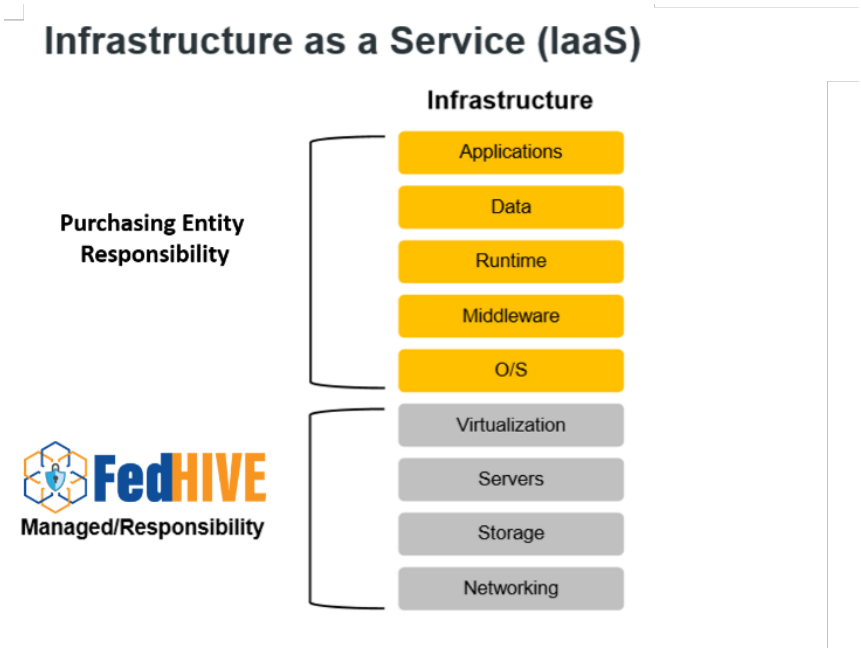
Platform as a Service (PaaS) – The FedHIVE PaaS Offering proposed for the NASPO MSA provides for the provision of customer-created or acquired applications. These applications are tested in the HRTec TDE then transferred to production where HRTec provisions, manages and controls the infrastructure and platform in support of customer/agency supplied, managed and controlled applications and data. **Exhibit 6C: HRTec FedHIVE PaaS Infrastructure** illustrates the division of management and control responsibilities of HRTec/FedHIVE and the customer/agency.

Exhibit 6C: HRTec FedHIVE PaaS Infrastructure



Infrastructure as a Service (IaaS) – The FedHIVE IaaS Offering provisions processing, storage, networks, and other fundamental computing resources for the consumer/agency. The customer/agency is able to deploy and run software that has been tested in the HRTec TDE and transferred to production where the customer/agency has responsibility for the operating systems and applications. HRTec will manage and control the underlying cloud infrastructure but the customer/agency has control over operating systems, storage, deployed applications. **Exhibit 6D: HRTec FedHIVE IaaS Infrastructure** illustrates the division of management and control responsibilities of HRTec/FedHIVE IaaS and the customer/agency.

Exhibit 6D: HRTec FedHIVE IaaS Infrastructure



Deployment Models

HRTec Cloud Service Offerings are high impact baseline protected offerings. To limit risk our offerings are only deployed in Private, Community, or a Private/Community Hybrid deployment models designed for the explicit purpose of serving the requirements of the customer/agency.

HRTec deploys/provisions all three service models within the FedHIVE infrastructure in the following deployment models:

- **Private cloud.** When required a private cloud enclave can be provisioned for exclusive use by a customer/agency within the FedHIVE IaaS.
- **Community cloud.** The FedHIVE cloud infrastructure is primarily provisioned to support cloud enclaves for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). Current community enclaves include Defense (DoD only customers/agencies) and Government (Federal, State, Local and Tribal customers/agencies).
- **Hybrid cloud.** The FedHIVE cloud infrastructure can support a composition of private and community cloud infrastructures that remain unique entities, but are bound together by FedHIVE standardized and proprietary technology that enables data and application portability.

6.2. Subcontractors (RFP Section 8.2)

8.2.1. - Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly

qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

HRTec is **fully capable and qualified** to deliver cloud solutions under all proposed service categories and delivery models in support of the NASPO ValuePoint Cloud Solutions MSA without assistance from or use of subcontractors. The HRTec Executive Management Team with input from our information systems security officer and compliance manager conducted a thorough risk assessment and determined that it is imperative that our high impact cloud solutions are provided directly and solely by HRTec's ISWF. Direct provision by HRTec of all systems and services reduces/mitigates corporate and customer/agency risks and complexity inherent with outsourcing systems and solutions to subcontractors.

8.2.2. - Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Not Applicable.

8.2.3 - If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

Not Applicable.

6.3. Working with Purchasing Entities (RFP Section 8.3)

8.3.1. - Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

HRTec's implemented Event/Incident Response Plan (EIRP) and Event/Incident Communications Plan both provide roles and responsibilities for all HRTec personnel. The plans address or assigns specific individuals to key roles. This ensures each Response Team member fully understands their role and responsibility regarding any event or potential incident that may or may not be a Data Breach. The plans also define events and incidents; not all events are incidents, but all incidents are events. Response times are measured beginning immediately upon identification of a potential event to when an incident is declared. Communication by HRTec takes multiple forms that include email, telephone, text messaging, help desk ticketing, and website reporting forms. The communications method for customers/agencies is defined within the customer/agency contract, the statement of work (SOW) or performance work statement (PWS), and SLA established for contracted services. HRTec's plans, policies, and procedures are developed and maintained in accordance with NIST SP 800-61 Computer Security Incident Handling Guide, NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response, US-CERT

Federal Incident Notification Guidelines (2015), FedRAMP INCIDENT COMMUNICATION PROCEDURE Version 3.0, FedRAMP Continuous Monitoring Strategy Guide Version 3.2, and the Department of Defense Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) Revision 1. HRTec reviews all policies, plans, and procedures annually at a minimum, or at time of an After-Action Review (AAR) as a result from an exercise, testing of plans, an event, or an incident. All changes are reviewed by HRTec Executive Leadership and the Audit Team.

SLA Para 8. Data Compromise Response

8.1. HRTec will report, either orally or in writing, to the [Customer/Agency] any Data Compromise involving the [Customer/Agency] or End User Data, or circumstances that could have resulted in unauthorized access to or disclosure or use of the [Customer/Agency] or End User Data, not authorized by this Agreement or in writing by the [Customer/Agency], including any reasonable belief that an unauthorized individual has accessed the [Customer/Agency] or End User Data. HRTec will make the report to the [Customer/Agency] immediately upon discovery of the unauthorized disclosure, but in no event more than seventy-two (72) hours after HRTec reasonably believes there has been such unauthorized use or disclosure. Oral reports by HRTec regarding Data Compromises will be reduced to writing and supplied to the [Customer/Agency] as soon as reasonably practicable, but in no event more than seventy-two (72) hours after oral report.

8.2. Immediately upon becoming aware of any such Data Compromise, HRTec will fully investigate the circumstances, extent and causes of the Data Compromise, and report the results to the [Customer/Agency] and continue to keep the [Customer/Agency] informed daily of the progress of its investigation until the issue has been effectively resolved.

8.3. HRTec's report discussed herein will identify:

(a) the nature of the unauthorized use or disclosure
(b) the [Customer/Agency] or End User Data used or disclosed
(c) who made the unauthorized use or received the unauthorized disclosure (if known)
(d) what HRTec has done or will do to mitigate any deleterious effect of the unauthorized use or disclosure
(e) what corrective action HRTec has taken or will take to prevent future similar unauthorized use or disclosure.

8.4. Within sixty (60) calendar days of the date HRTec becomes aware of any such Data Compromise, HRTec shall have completed implementation of corrective actions to remedy the Data Compromise, restore the [Customer/Agency] access to the Services as directed by the [Customer/Agency], and prevent further similar unauthorized use or disclosure.

8.5. HRTec will cooperate fully with the [Customer/Agency] investigation of and response to any such Data Compromise incident.

8.6. Except as otherwise required by law, HRTec will not provide notice of the incident directly to the persons whose Data were involved, regulatory agencies, or other entities, without prior written permission from the [Customer/Agency].

SLA Appendix A, Article 6 – Breaches of Protected Information

A. Definition. For purposes of this article, a "Breach" has the meaning given to it under relevant [State] or federal law, for example, California Civil Code Section 1798.29, California Health and Safety Code Section 1280.15, etc.

B. Reporting of Breach: HRTec shall report any confirmed or suspected Breach to [Customer/Agency] immediately upon discovery, both orally and in writing, but in no event more than two (2) business days after HRTec reasonably believes a Breach has or may have occurred. HRTec's report shall identify: (i) the nature of the unauthorized access, use or disclosure, (ii) the Protected Information accessed, used or disclosed, (iii) the person(s) who accessed, used and disclosed and/or received Protected Information (if known), (iv) what HRTec has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action HRTec has taken or will take to prevent future unauthorized access, use or disclosure. HRTec will provide such other information, including a written report, as reasonably requested by the

[Customer/Agency]. In the event of a suspected Breach, HRTec shall keep the [Customer/Agency] informed regularly of the progress of its investigation until the uncertainty is resolved.
C. Coordination of Breach Response Activities: In the event of a Breach, HRTec will: Immediately preserve any potential forensic evidence relating to the breach, and remedy the breach as quickly as circumstances permit:
1. Promptly (within 3 business days) designate a contact person to whom the [Customer/Agency] will direct inquiries, and who will communicate HRTec responses to the [Customer/Agency] inquiries
2. As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore [Customer/Agency] service(s) as directed by the [Customer/Agency], and undertake appropriate response activities
3. Provide status reports to the [Customer/Agency] on Breach response activities, either on a daily basis or a frequency approved by the [Customer/Agency]
4. Coordinate all media, law enforcement, or other Breach notifications with the [Customer/Agency] in advance of such notification(s), unless expressly prohibited by law
5. Make all reasonable efforts to assist and cooperate with the [Customer/Agency] in its Breach response efforts
6. Ensure that knowledgeable HRTec staff are available on short notice, if needed, to participate in [Customer/Agency]-initiated meetings and/or conference calls regarding the Breach.

8.3.2 - Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

HRTec Cloud Service Offerings are high impact baseline protected offerings. To limit risk our offerings are only deployed in Private, Community, or a Private/Community Hybrid deployment models designed for the explicit purpose of serving the requirements of the customer/agency. Therefore, HRTec does not permit nor engage in marketing or allow adware within the FedHIVE boundary, nor do we permit use of any software not explicitly supporting the confidentiality, integrity, availability, and protection of the customer/agency authorized services.

8.3.3 - Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

HRTec maintains a Test and Development Environment (TDE) for verification and validation of requested changes and user test/staging prior to promotion and implementation into production environments. The TDE is configured to be an identical representation of the user's production environment within the associated private or community enclaves.

8.3.4 - Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable

All HRTec application are developed to meet the requirements of Section 508, an amendment to the United States Workforce Rehabilitation Act of 1973, which is the federal law mandating that all electronic and information technology developed, procured, maintained, or used by the federal government be accessible to people with disabilities. In addition, we ensure compliance with the Americans with Disability Act and Web Content Accessibility Guidelines (WCAG) 2.0 AA, as applicable.

SLA Para 3.2 All Services, including any Support and Training requirements addressed herein, provided by HRTec that are provided online will be Americans with Disability Act and Web Content Accessibility Guidelines (WCAG) 2.0 AA compliant, as applicable.

SLA Para 15.4 (d) In addition to HRTec's obligations under Section 3.2 of this Agreement, HRTec provided telephone technical support will be compliant with Section 508 of the Rehabilitation Act.

8.3.5 - Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

HRTec's applications are tested for accurate content delivery across all current browser technologies (such as Internet Explorer, Firefox, Chrome, and Safari). All browsers should be configured to TLS 1.1 or higher for security compliance.

SLA Para 12.3 HRTec warrants that the minimum technical requirements for access to and operation of the Cloud Computing Services are [LIST HERE APPLICABLE REQUIREMENTS, E.G. MICROSOFT INTERNET EXPLORER VERSION ## (OR HIGHER), FIREFOX VERSION ## (OR HIGHER), ETC. ALSO, CONSIDER ANY APPLICABLE REQUIREMENTS FOR ACCESS/USE BY MOBILE DEVICES]. If future Enhancements to the Cloud Computing Services require use of newer versions of these web browsers, HRTec will provide a minimum of sixty (60) days written notice to the [Customer/Agency] prior to implementing such Enhancements. Additional technical requirements for complete operation of all functionality of the Cloud Computing Services include [INSERT HERE ANY OTHER TECHNICAL REQUIREMENTS NECESSARY TO ACCESS AND/OR OPERATE THE SERVICES].

8.3.6 - Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Immediately upon contract award the HRTec Contract Manager will contact the Purchasing Entity to schedule a post award conference. This conference will serve as the project kick-off meeting and HRTec will brief the Purchasing Entity's team on the proposed draft provisioning plan and schedule, as well as establish a communication and data collection plan to ensure efficient and effective project interactions. Specific topics will include the confidentiality, availability, and integrity requirements and identification of sensitive or personal information storage or usage subject to current laws, rules, or regulations and compliance obligations.

8.3.7 - Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

HRTec approaches project schedules and work plans as unique to each customer engagement. Generally, HRTec generally follows a five-step approach:

- Project conception and initiation
- Project definition and planning
- Project launch or execution
- Project performance and control
- Project closeout

Project scheduling is established with deliverables and milestones. For development projects HRTec's development lifecycle incorporates Open Web Application Security Project (OWASP) concepts and processes to ensure security inclusion throughout the development lifecycle.

SLA Para 17 Transition Assistance

17.1 HRTec will develop, provide and implement the following transition assistance ("Transition Assistance") to support the [Customer/Agency] successful and uninterrupted transition from its current solution, or other solution in this area, to HRTec's Cloud Computing Services. Transition Assistance will be provided by HRTec as detailed below at no additional cost to the [Customer/Agency]. Transition assistance will be provided by HRTec at mutually agreeable dates and times, but no later than ten (10) calendar days following the Effective Date of this Agreement.
[INCLUDE DESCRIPTION, FREQUENCY AND TIMING OF ANY NEGOTIATED TRANSITION ASSISTANCE HERE. EXAMPLE TEXT IS BELOW].

17.2 Within no more than ten (10) calendar days after the Effective Date of this Agreement, HRTec will provide qualified individuals to a) implement the Cloud Computing Services, and b) assist in testing of the Cloud Computing Services to ensure that they are functioning in accordance with the terms of this Agreement.

17.3 HRTec's Project Manager shall coordinate with the [Customer/Agency] Project Manager, and they shall develop a mutually agreeable installation plan and schedule for the assistance provided above.

17.4 The installation plan shall provide for: a) The timely and successful integration of HRTec software, applications and Cloud Computing Services with the [Customer/Agency] existing identity management and access management systems [SPECIFY EXISTING IMAM SYSTEMS HERE AS APPROPRIATE.]; b) The timely and successful integration with specified [Customer/Agency] applications [SPECIFY APPLICATIONS HERE]; c) The availability of and support for the Cloud Computing Services via specified [Customer/Agency] and End User devices including mobile devices [SPECIFY DEVICES HERE]; and d) the [Customer/Agency] ability to, directly or through instructions to HRTec, create, modify, suspend, eliminate, assign aliases for, and internally delegate the administration of, individual and group accounts created as part of HRTec's provision of Cloud Computing Services.

17.5 In connection with HRTec's Transition Assistance, the [Customer/Agency] will provide information, Data, computer access and time, work space, forms, data entry and telephone service and personnel reasonably necessary to assist HRTec with the transition consistent with [Customer/Agency] policies and procedures.

17.6 If HRTec receives customer deliverables per the approved transition plan and fails to meet the target date for completion of transition, HRTec will credit the [Customer/Agency] day for day Services fees for every business day the transition is late. If HRTec misses the target date by more than thirty (30) calendar days, the [Customer/Agency] may terminate the Agreement..

8.3.8. - The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.
- How Offeror will maintain discounts at the levels set forth in the contract.
- How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.
- How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

HRTec anticipates that we can use the same approach that has been successful for our GSA IT Schedule 70 contract new offerings. HRTec has held a very successful GSA Schedule Contract for nearly twenty years; with new offerings being added over the years to enhance the contract offerings through catalog updates and submitted per the GSA guidelines for adding mew solutions and/or services.

- HRTec will conduct a services gap analysis during our periodic review of existing requirements and identified new service requirements. The review and analysis will be provided to the State of Utah, as the lead state, for review and acceptance prior to listing any new services. This process will ensure new additions with accompanying terms and conditions will not diminish or weaken existing terms and conditions.
- During the review process, all pricing discounts are reviewed and validated to the levels of the contract
- Notifications to Purchasing Entities for service updates are detailed within our SLA document please refer to the SLA excerpt from paragraphs 15.6 and 15.7 below.
- HRTec staff test service changes prior to rollout to identify potential operations that may be negatively impacted within our Test and Development environment. Should impacts be identified, HRTec's Contract Manager will contact the specific Purchasing Entity affected with the service change. The HRTec Contract Manager will work with the Purchasing Entity to develop a plan to mitigate and correct identified issues. Once the plan is developed and executed, another round of testing will be conducted to ensure there is no further impact on the operations prior to release into production.

SLA Para 15.6 Enhancements
The following provisions shall set forth HRTec's obligations to provide Enhancements:

(a) HRTec will generally enhance and improve the Cloud Computing Services for as long as the [Customer/Agency] elects to receive and pays for the Cloud Computing Services.
(b) HRTec will provide to the [Customer/Agency] during the Agreement term, (1) any and all Enhancements which it develops with respect to the Cloud Computing Services; (2) any and all Enhancements required by federal or state governmental, or professional regulatory mandates related to [Customer/Agency] use of the Cloud Computing Services; and (3) the Documentation associated with any Enhancements.
(c) HRTec will provide Enhancements to the [Customer/Agency] upon their general release and no later than the time when the first five percent (5%) of HRTec's customers receive those Enhancements.
(d) Except as otherwise provided in a signed addendum to this Agreement, nothing herein shall obligate HRTec to enhance the Cloud Computing Services in any particular respect or on any particular date. The decision as to whether and/or when, to enhance the Cloud Computing Services will be within HRTec's discretion.

SLA Para 15.7 Product Changes
HRTec will provide the [Customer/Agency] with sixty (60) calendar days advance written notice of proposed product changes as well as product road maps relating to the Cloud Computing Services provided to the [Customer/Agency] under this Agreement.

6.4. Customer Service (RFP Section 8.4)

8.4.1. - Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA).

HRTec's prides it self on the success of our customer service and support. The HRTec staff is experienced and very knowledgeable of the HRTec service offerings. Escalation is addressed within the SLA. As a single stack provider, HRTec does not need to bring in other vendors to support application issues. HRTec has strong working relations with its hardware vendors and 24x7-4-hour response should additional escalation be required to resolve an issue. Customers have the option to supply feedback on their experience

SLA Section 15. Technical Support

15.5. The following provisions shall be applicable to the correction of Services errors:

(a) If the [Customer/Agency] detects what it considers to be an error in the Cloud Computing Services which causes it not to conform to, or produce results in accordance with, the Documentation, then the [Customer/Agency] shall by telephone or e-mail notify HRTec of the error.

(b) HRTec will deliver to the [Customer/Agency] and keep current a list of persons and telephone numbers (the "HRTec Calling List") for [Customer/Agency] to contact in order to obtain corrections of Cloud Computing Services errors. The HRTec Calling List shall include: 1) the first person to contact if a question arises or problem occurs; and 2) the persons in successively more responsible or qualified positions to provide the answer or assistance desired. If HRTec does not respond promptly to any request by the [Customer/Agency] for telephone consultative service, The [Customer/Agency] may attempt to contact the next more responsible or qualified person on the HRTec Calling List until contact is made and a designated person responds to the call.

(c) HRTec shall respond within two (2) hours to the [Customer/Agency] initial request for assistance in correcting or creating a workaround for a Cloud Computing Services error. HRTec's response shall include assigning fully-qualified technicians to work with the [Customer/Agency] to diagnose and correct or create a workaround for the Cloud Computing Services error and notifying the [Customer/Agency] representative making the initial request for assistance of HRTec's efforts, plans for resolution of the error, and estimated time required to resolve the error.

(d) For Class 1 Errors, within twenty-four (24) hours after the [Customer/Agency] first reports the error, HRTec will provide a correction or workaround acceptable to the [Customer/Agency]. HRTec's correction process will include assigning fully-qualified technicians to work with the [Customer/Agency] without interruption or additional charge.

(e) If HRTec fails to provide a reasonable correction or workaround for a Class 1 Error within twenty-four (24) hours, HRTec shall provide a price adjustment reflecting the reduction of value the [Customer/Agency] will incur as a result of the Class 1 Error and not as a penalty or compensation for damage, the sum of 1/365 of the technical support fees, expressed as an annual charge, for each additional day or part thereof that HRTec fails to provide a reasonable correction or workaround for the Class 1 Error. HRTec will provide such payment in the form of a check provided to the [Customer/Agency] no later than the tenth (10th) business day following the month in which failure to correct occurred.

(f) The Project Managers, or such persons as otherwise designated by the [Customer/Agency] and HRTec, shall serve as said parties' contacts for all communications relating to technical support. Each party may change its own contact person by written notice to the other party.

8.4.2 - Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

c. Customer Service Representative will respond to inquiries within one business day.

d. You must provide design services for the applicable categories.

e. You must provide Installation Services for the applicable categories.

The HRTec Contract Manager is responsible for ensuring all customer service requirements are met throughout the lifecycle of each customer/agency provisioned offering(s). This includes but is not limited to:

- Assigning a lead customer service representative to each customer/agency.
- Ensuring complete contact information for customer support and the assigned lead is provided and kept current via customer portals and appropriate correspondence
- Providing Customer support is available by phone from daily 7am to 6pm in Continental US time zones, and by email, and service ticket 24/7/365.
- Ensuring Customer support responds to all inquiries within one business day
- Ensuring Design services are provided for all new requirements via the transition support
- Enforcing HRTec requirements for installation services per FedHIVE security policies and procedures.

SLA Section 15. Technical Support

15.5. The following provisions shall be applicable to the correction of Services errors:

(a) If the [Customer/Agency] detects what it considers to be an error in the Cloud Computing Services which causes it not to conform to, or produce results in accordance with, the Documentation, then the [Customer/Agency] shall by telephone or e-mail notify HRTec of the error.

(b) HRTec will deliver to the [Customer/Agency] and keep current a list of persons and telephone numbers (the "HRTec Calling List") for [Customer/Agency] to contact in order to obtain corrections of Cloud Computing Services errors. The HRTec Calling List shall include: 1) the first person to contact if a question arises or problem occurs; and 2) the persons in successively more responsible or qualified positions to provide the answer or assistance desired. If HRTec does not respond promptly to any request by the [Customer/Agency] for telephone consultative service, The [Customer/Agency] may attempt to contact the next more responsible or qualified person on the HRTec Calling List until contact is made and a designated person responds to the call.

(c) HRTec shall respond within two (2) hours to the [Customer/Agency] initial request for assistance in correcting or creating a workaround for a Cloud Computing Services error. HRTec's response shall include assigning fully-qualified technicians to work with the [Customer/Agency] to diagnose and correct or create a workaround for the Cloud Computing Services error and notifying the [Customer/Agency] representative making the initial request for assistance of HRTec's efforts, plans for resolution of the error, and estimated time required to resolve the error.

(d) For Class 1 Errors, within twenty-four (24) hours after the [Customer/Agency] first reports the error, HRTec will provide a correction or workaround acceptable to the [Customer/Agency]. HRTec's correction process will include assigning fully-qualified technicians to work with the [Customer/Agency] without interruption or additional charge.

(e) If HRTec fails to provide a reasonable correction or workaround for a Class 1 Error within twenty-four (24) hours, HRTec shall provide a price adjustment reflecting the reduction of value the [Customer/Agency] will incur as a result of the Class 1 Error and not as a penalty or compensation for damage, the sum of 1/365 of the technical support fees, expressed as an annual charge, for each additional day or part thereof that HRTec fails to provide a reasonable correction or workaround for the Class 1 Error. HRTec will provide such payment in the form of a check provided to the [Customer/Agency] no later than the tenth (10th) business day following the month in which failure to correct occurred.

(f) The Project Managers, or such persons as otherwise designated by the [Customer/Agency] and HRTec, shall serve as said parties' contacts for all communications relating to technical support. Each party may change its own contact person by written notice to the other party.

6.5. Security of Information (RFP Section 8.5)

8.5.1. - Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

HRTec manages and enhances the native encryption functionality Microsoft BitLocker on Windows platforms through automated policy. Management of native encryption provides a zero-day compatibility with Microsoft Windows patches, upgrades, and firmware updates; while additionally providing administrators the ability to manually import recovery keys where users have already enabled BitLocker. HRTec's encryption security solution is FIPS 140-2 and Common Criteria EAL2+ certified and accelerated with the Intel Advanced Encryption Standard—New Instructions (Intel AES-NI) set. Data retention and disposal is conducted per HRTec SLA paragraph 9 Data Retention and Disposal and paragraph 10 Data Transfer upon Termination or Expiration.

SLA Para 5. Data Privacy

5.1 HRTec will use [Customer/Agency] Data and End User Data only for fulfilling its duties under this Agreement and for the [Customer/Agency]'s and its End User's sole benefit and will not share such Data with or disclose it to any Third Party without the prior written consent of the [Customer/Agency] or as otherwise required by law. By way of illustration and not of limitation, HRTec will not use such Data for HRTec's own benefit and will not engage in "data mining" of [Customer/Agency] or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the [Customer/Agency].

5.2 All [Customer/Agency] and End User Data will be stored on servers located solely within the Continental United States.

5.3 HRTec will provide access to [Customer/Agency] and End User Data only to those HRTec employees, contractors and subcontractors ("HRTec Staff") who need to access the Data to fulfill HRTec's obligations under this Agreement. HRTec will ensure that, prior to being granted access to the Data, HRTec Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

5.4 The [Customer/Agency] represents that it is subject to [List all data privacy regulations, laws and policy requirements imposed on the Customer/Agency, it's End Users and Suppliers] (e.g. all applicable federal and state laws restricting the access, use and disclosure of Protected Information and all the terms and conditions contained in Appendix A).

SLA Para 6. Data Security and Integrity

6.1. All HRTec facilities used to store and process [Customer/Agency] and End User Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such Data from unauthorized access, destruction, use, modification, or disclosure. Such measures will be no less protective than those used to secure HRTec's own Data of a similar type, and in no event less than reasonable in view of the type and nature of the Data involved.

6.2. HRTec shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Cloud Computing Services to the [Customer/Agency] in a manner that is, at all times during the term of this Agreement, at a level equal to or more stringent than those specified in Exhibit ___, which is incorporated herein by reference.

6.3. Without limiting the foregoing, HRTec warrants that all [Customer/Agency] Data and End User Data will be encrypted in transmission (including via web interface) and in storage at a level equivalent to or stronger than 256-bit level encryption

6.4. HRTec shall at all times use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting methods [List additional specifically required security mechanisms here as appropriate.] in providing Services under this Agreement.

6.5. HRTec will configure the Services to filter spam while permitting communications from Third Party Internet Protocol addresses identified by the [Customer/Agency] as legitimate, as specified in Exhibit ___.

6.6. Prior to the Effective Date of this Agreement, HRTec will at its expense conduct or have conducted the following, and thereafter, HRTec will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise:
(a) A Third-Party Assessment Organization (3PAO) audit of Supplier's security policies, procedures and controls
(b) Certification under FedRAMP and/or Cloud Security Alliance Security Trust and Assurance Registry (CSA STAR) attestation and certification
(c) A vulnerability scan, performed by a HRTec and [Customer/Agency]-approved Third Party scanner, of HRTec's systems and facilities that are used in any way to deliver Cloud Computing Services under this Agreement

(d) A formal penetration test, performed by the process and qualified personnel approved by HRTec and [Customer/Agency], of HRTec's systems and facilities that are used in any way to deliver Cloud Computing Services under this Agreement.

6.7. HRTec will provide the [Customer/Agency] the reports or other documentation resulting from the above audits, certifications, scans and tests within seven (7) business days of HRTec's receipt of such results.

6.8. Based on the results of the above audits, certifications, scans and tests, HRTec will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement, and provide the [Customer/Agency] with written evidence of remediation.

6.9. The [Customer/Agency] may require, at its expense, that HRTec perform additional audits and tests, the results of which will be provided to the [Customer/Agency] within seven (7) business days of Supplier's receipt of such results.

6.10. HRTec shall protect the [Customer/Agency] and End User Data against deterioration or degradation of Data quality and authenticity, including, but not limited to annual Third-Party Data integrity audits. HRTec will provide the [Customer/Agency] the results of the above audits, along with Supplier's plan for addressing or resolving any shortcomings identified by such audits, within seven (7) business days of HRTec's receipt of such results

SLA Para 9. Data Retention and Disposal

9.1. HRTec will retain Data in an End User's account, including attachments, until the End User deletes them or for the time period mutually agreed to by the parties in this Agreement.

9.2. Using appropriate and reliable storage media, HRTec will regularly backup [Customer/Agency] and End User Data and retain such backup copies for a minimum of twelve (12) months.

9.3. At the [Customer/Agency] election, HRTec will either securely destroy or transmit to the [Customer/Agency] repository any backup copies of the [Customer/Agency] and/or End User Data. HRTec will supply the [Customer/Agency] a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.

9.4. HRTec will retain logs associated with End User activity for a minimum of twelve (12) months.

9.5. HRTec will immediately place a "hold" on Data destruction or disposal under its usual records retention policies of records that include the [Customer/Agency] and End User Data, in response to an oral or written request from the [Customer/Agency] indicating that those records may be relevant to litigation that the [Customer/Agency] reasonably anticipates. Oral requests by the [Customer/Agency] for a hold on record destruction will be reduced to writing and supplied to HRTec for its records as soon as reasonably practicable under the circumstances. The [Customer/Agency] will promptly coordinate with HRTec regarding the preservation and disposition of these records. HRTec shall continue to preserve the records until further notice by the [Customer/Agency].

SLA Para 10. Data Transfer upon Termination or Expiration

10.1 Upon termination or expiration of this Agreement, HRTec will ensure that all [Customer/Agency] and End User Data are securely transferred to the [Customer/Agency], or a Third Party designated by the [Customer/Agency], within thirty (30) calendar days, all as further specified in the technical specifications attached as Exhibit ___. HRTec will ensure that such migration uses facilities and methods that are compatible with the relevant systems of the [Customer/Agency], and that the [Customer/Agency] will have access to the [Customer/Agency] and End User Data during the transition.

10.2 HRTec shall implement its contingency and/or exit plans and take all necessary actions to provide for an effective and efficient transition of service with minimal disruption to the [Customer/Agency]. HRTec will work closely with its successor to ensure a successful transition to the new service and/or equipment, with minimal Downtime and effect on the [Customer/Agency], all such work to be coordinated and performed no less than ninety (90) calendar days in advance of the formal, final transition date.

8.5.2 - Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

HRTec has implemented policies and procedures that address compliance with data privacy and security. As part of HRTec's FedRAMP authorization compliance with all applicable laws and regulations related to data privacy and security is audited monthly. Some of the administrative safeguards include employee background checks, annual training requirements for data privacy, information and physical security, a progressive disciplinary policy, physical and logical access limitations to the least privileged level are a few. Physical safeguards include two factor authentication with Personal Identity Verification (PIV) cards meeting Federal Information Processing Standards Publication 201 (FIPS 201) and Homeland Security Presidential Directive-12 (HSPD-12) requirements, a PIN code, or biometric identification; password requirements enforced by policy that require complexity, length and frequent changing; encryption of all data at rest or in motion, and continuous monitoring of all activity through automated and manual scans to detect abnormal behavior.

SLA Para 14. Compliance with Applicable Laws and [Customer/Agency] Policies

HRTec will comply with all applicable laws in performing Cloud Computing Services under this Agreement. Any HRTec personnel visiting the [Customer/Agency] facilities will comply with all applicable [Customer/Agency] policies regarding access to, use of, and conduct within such facilities. [Customer/Agency] will provide copies of such policies to HRTec upon request.

8.5.3 - Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

HRTec employs and enforces a least privileged access policy for all internal users; this approach is also highly suggested to all Purchasing Entities through the enacted NIST 800-53 controls inherited from the HRTec provided solution. The ISWF reviews and analyzes log files and records produced by our FedRAMP approved security and management tools to ensure least privilege is effective. Least privilege is validated as part of our FedRAMP required monthly audits of HRTec Systems. Additionally, all access activity for ISWF on HRTec production systems is managed by a Privileged Access Management (PAM) tool that provides session recording with date, time and user recorded. Additional network scanning monitors behavioral activities and reports all abnormal behavior as an alert.

SLA Para 5. Data Privacy

5.1 HRTec will use [Customer/Agency] Data and End User Data only for fulfilling its duties under this Agreement and for the [Customer/Agency]'s and its End User's sole benefit and will not share such Data with or disclose it to any Third Party without the prior written consent of the [Customer/Agency] or as otherwise required by law. By way of illustration and not of limitation, HRTec will not use such Data for HRTec's own benefit and will not engage in "data mining" of [Customer/Agency] or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the [Customer/Agency].

5.2 All [Customer/Agency] and End User Data will be stored on servers located solely within the Continental United States.

5.3 HRTec will provide access to [Customer/Agency] and End User Data only to those HRTec employees, contractors and subcontractors ("HRTec Staff") who need to access the Data to fulfill HRTec's obligations under this Agreement. HRTec will ensure that, prior to being granted access to the Data, HRTec Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

5.4 The [Customer/Agency] shall represents that it is subject to [List all data privacy regulations, laws and policy requirements imposed on the Customer/Agency, it's End Users and Suppliers] (e.g. all applicable federal and state laws restricting the access, use and disclosure of Protected Information and all the terms and conditions contained in Appendix A).

6.6. Privacy and Security (RFP Section 8.6)

HRTec's compliance to privacy and security is managed through established policies and procedures that apply to all service offerings (IaaS, PaaS, & SaaS). Purchasing Entities (customers/agencies) will in some cases inherit HRTec privacy and security controls that will exceed the specific requirements established by the customer/agency. In many cases there will be a shared responsibility on the part of the customer/agency and HRTec. Likewise, a customer/agency may be responsible for defining the privacy or security controls as their sole responsibility. All responsibilities inherited, shared, or customer /agency provided are identified and implemented based on the specific service offering, SLA, and/or the contract for services.

8.6.1. - Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in **Attachment D**, including supporting the different types of data that you may receive.

HRTec provides multiple community enclaves within its boundaries. The enclaves are divided by customer vertical State, Local Government & Education (SLED); FedRAMP with two sub enclaves Civilian Federal (CIV), Defense (DEF); and Commercial & Corporate (COM). Within each dedicated enclave tenant separation is ensured based on the deployment model for that tenant. Each enclave is audited monthly for compliance with applicable computer security controls, configurations, vulnerability, and physical access.

8.6.2 - Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

HRTec's data centers operate under the following standards, certifications, and regulations:

- Federal Risk and Authorization Management Program (FedRAMP)
  - High Baseline Ready
  - High Baseline Joint Authorization Board Provisional Authority to Operate (JAB P-ATO) - pending
- Statement on Standards for Attestation Engagements (SSAE) No. 18
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Homeland Security Presidential Directive-12 (HSPD-12)

- Federal Information Processing Standard (FIPS) Publications
    - 140-2, 199, 200, 201-1, & 201-2
- Federal Information Security Management Act (FISMA)
- National Institute of Standards and Technology (NIST) Special Publications (SP)
    - 800-53r4, 800-122, 800-137, 800-157, 800-171
- Defense Information Systems Agency (DISA) Cloud Service Provider (CSP)
    - Cloud Service Offering (CSO) Level 4/5 with privacy overlay – pending.

8.6.3 - Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

HRTec has developed and implemented a series of comprehensive plans policies and procedures which are the basis and defines HRTec's security practices. Policies and plans are reviewed annually at a minimum; maintaining the strength, viability, and effectiveness of HRTec's security practices.

Policies and plans supporting and defining HRTec's security practices include the following:

- HRTec Information Security Program Plan
- HRT-Secure Cloud Service System Security Plan
- System Security Plan (SSP); this plan defines the current security posture for the HRT-Secure Cloud Service as it operates under. The plan is supported by an extensive library of policies and procedures to implement the SSP. The SSP captures the system environment, system responsibilities, and the current status, implementation, and responsibility for all applicable High baseline controls.

The environment additionally is protected by a multi-layered security for logical and physical security. HRTec utilizes several advanced security and management tools with overlapping capabilities in maintenance, monitoring, detection, prevention and remediation. As part of the SSP and HRTec's policies and procedures a Continuous Monitoring program is utilized to maintain the vigilance and responsiveness of threat protection. The continuous monitoring is not only standing by for automated system alerts. HRTec's staff is continually validating scans and reports produced as part of ongoing security analysis.

As described in section 8.6.1, the physical separation of enclaves is the first separation of customers. Additionally, the delivery model chosen by the customer is another and identifies separations of virtual machines. HRTec additionally provides logical separations with the deployments of secure virtual private networks (VPNs) and secure virtual local area networks (VLANs) aiding protection of customer data and applications.

HRTec additionally in support of data and application protection conducts regular penetration testing. This penetration testing simulates multiple attack vectors: external network information gathering and discovery attack, external target system attack, target system to management system attack, and tenant to tenant attack. This testing aids HRTec with additional situational awareness of potential vulnerabilities

8.6.4 - Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc.).

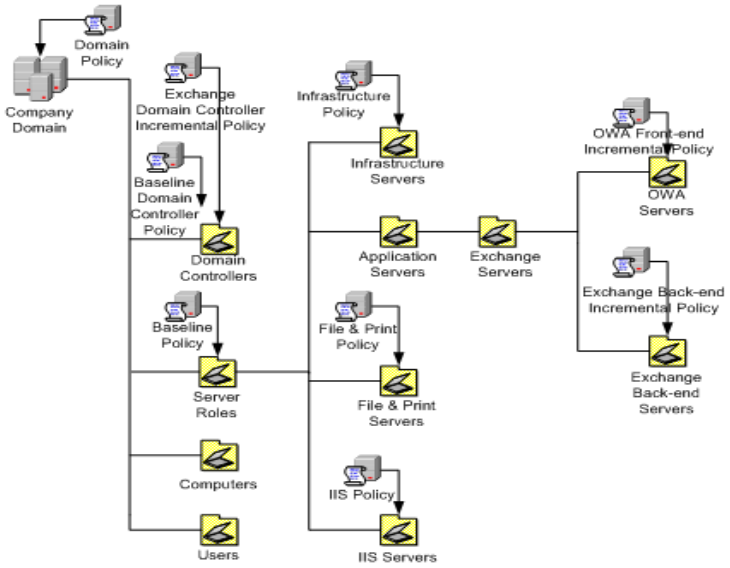
HRTec policies and procedures address multiple areas regarding data confidentiality standards and practices. **Exhibit 6D: HRTec Policies, Procedures and Plans** provides for a list of applicable policies, procedures and plans.

Exhibit 6D: HRTec Policies, Procedures and Plans

HRTec Policies, Procedures, and Plans	Policy Number or Version	Revision Date
HRTec Access Control Policy	05-P-AC-001	05/23/2018
HRTec Audit & Accountability Policy	05-P-AU-001	11/08/2017
HRTec Awareness & Training Policy	05-P-AT-001	09/07/2017
HRTec Contingency Planning Policy & Procedure	05-P-CP-001	06/03/2018
HRTec Enterprise Configuration Management Policy	05-P-CM-001	11/03/2017
HRTec Enterprise Configuration Management Plan	Version 3.1	11/07/2017
HRTec Identification & Authentication Policy	05-P-IA-001	06/23/2017
HRTec Incident Response Policy	05-P-IR-001	06/23/2017
HRTec Information System Security Plan	Version 3.1	08/04/2017
HRTec Maintenance Policy	05-P-MA-001	06/23/2017
HRTec Media Protection Policy	05-P-MP-001	05/23/2018
HRTec Monthly Security Audit Plan	Version 2.0	05/01/2018
HRTec Personnel Security Policy & Procedures	05-P-PS-001	07/13/2017
HRTec Physical & Environmental Protection Policy & Procedures	05-P-PE-001	07/13/2017
HRTec Security Assessment & Authorization	05-P-CA-001	11/16/2017
HRTec System & Communications Protection Policy	05-P-SC-001	04/23/2018
HRTec System & Information Integrity Policy	05-P-SI-001	08/17/2017

HRTec's practices to data confidentiality start with access control. HRTec enforces a least privileged approach. This is established through Active Directory (AD) and group policy enforcement. HRTec's AD is organized into multiple organizational units (OU) **Exhibit 6E: Sample Active Directory Organizational Unit Structure** depicts this structure or approach:

Exhibit 6E: Sample Active Directory Organizational Unit Structure



This diagram does not reflect the actual nature of HRTec's (as this information is highly sensitive and propriety) actual OU structure, it does identify the general points where group policy does apply. The OU structure provides roles and access for each employee. These define which employee inherits the authorizations and access rights to the infrastructure, platforms, databases, and applications. Privileged account access is further restricted through the deployment of a Privileged Account Management (PAM) system. The PAM provides all access to the infrastructure and the Test and Development Environment; complete management of the 256-bit encrypted passwords for each device; and full session recording.

HRTec's baseline configurations include the use of data encryption for data at rest and data in motion. HRTec's data encryption meet the requirements of FIPS PUB 140-2 Security Requirements for Cryptographic Modules at Security Level 4 and minimally Common Criteria Evaluation Assurance Level EAL4.

Identity Management for access to HRTec infrastructure or systems is accomplished through a series of two factor authentication for both logical and physical access. HRTec employees are issued personal identity verification PIV smart cards as the first form. These cards meet the requirements of NIST SP 800-63A Digital Identity Guidelines. The second factor is using a personal identification number (PIN), user defined password, or biometric. The authentication process is designed and managed in accordance with NIST SP 800-63-2 Electronic Authentication Guideline.

Maintenance and Media protection are best practice areas the ensure systems holding data are protected with patches and how to handle end of life or need for media. These policies provide the process HRTec employs as part of the overall data confidentiality and protection procedures. HRTec Awareness & Training Policy addresses personnel training requirements for privacy and confidentiality.

HRTec's Audit and Accountability policy and the supporting Monthly Security Audit Plan continuously reviews and validates HRTec's practices are meeting the requirements of data protection and confidentiality.

8.6.5 - Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRAMP High, FedRAMP Moderate, etc.), and certifications relating to data security, integrity, and other controls.

HRTec Secure Cloud Service Offerings met the requirements for the following third-party attestations, reports, security credentials, and certifications relating to data security, integrity, and other controls.

- **FedRAMP** High Baseline Authorization for IaaS and PaaS service offerings. HRTec is compliant and our Readiness Assessment Report was completed and submitted to FedRAMP by Blue Canopy our Third- Party Assessor Organization (3PAO) authorized by FedRAMP. HRTec will submit our Business Case prior to July 13, 2018, for full authorization by the FedRAMP Joint Authorization Board (JAB) to receive the JAB P-ATO Authorization for HRTec's IaaS and PaaS. Upon authorization, HRTec will be the fourth (4th) commercial provider for IaaS and PaaS and more notably the first Small Business with the capabilities and authorization to deliver CSO High Impact offerings.
- **CSA STAR**, HRTec is registered and self-assessed at LEVEL ONE. HRTec has engaged The PMC Group, LLC a cybersecurity and auditing consulting firm to complete LEVEL TWO CSA STAR Attestation, Certification, and LEVEL TWO CSA C-STAR Assessment. HRTec is positioned to become LEVEL THREE CSA STAR Continuous Monitoring once CSA completes development.
- Statement on Standards for Attestation Engagements No. 18 (SSAE 18)
- HIPAA (Health Insurance Portability and Accountability Act of 1996)
- Payment Card Industry Data Security Standard (PCI DSS).

8.6.6. - Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Log files are system generated and HRTec employs a security information and event management (SEIM) tool for the automated collection of log files. Typical log files collected include application, security, system, router logs, switch logs, and firewall logs. The SIEM tool provides specific automated analysis and graphical representation dashboard views for HRTec's Security Operations Center (SOC) personnel to monitor and analyze. In addition to the continuous monitoring by SOC personnel, HRTec's Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), and the HRTec Audit Team conduct a monthly security audit as part of our Continuous Security Monitoring Program for FedRAMP compliance.

All HRTec security personnel are required to maintain their annual security training in accordance with HRTec Awareness & Training Policy. As part of HRTec's FedRAMP Authorization, Monthly Security Audits, the maintenance of a Plan of Action and Milestones (POA&M), and complete inventory must be maintained and provided each month to the FedRAMP PMO to maintain authorization.

8.6.7. - Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

HRTec's architecture provides restricted visibility and access to data. Users externally accessing HRTec's application software do not have direct access to stored data. A user must login to a secure session with the proper credentials and be authenticated; then the application will securely be connected to stored data areas. HRTec software access is role based to restrict access or visibility to stored data. Tenant or customer/agency separation is logically accomplished through virtual machines (VM) for hosting servers, secure virtual local area networks (VLAN).

8.6.8. - Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

HRTec developed and has implemented an Event/Incident Response Plan (EIRP) and its companion HRTec Event/Incident Communication Plan (EICP). These plans provide the framework for stakeholder notifications. These plans ensure the response and communications requirements established by United States Computer Emergency Readiness Team (US-CERT) and the United States Department of Defense (DoD) Defense Industrial Base (DIB) Cyber Security Program are met. The US-CERT and DoD DIB requirements are included within FedRAMP High Impact Baseline requirements. HRTec's EIRP and EICP can accommodate any additional requirements established by a Purchasing Entity. HRTec's EIRP and EICP do include notification of any State-CERT when applicable.

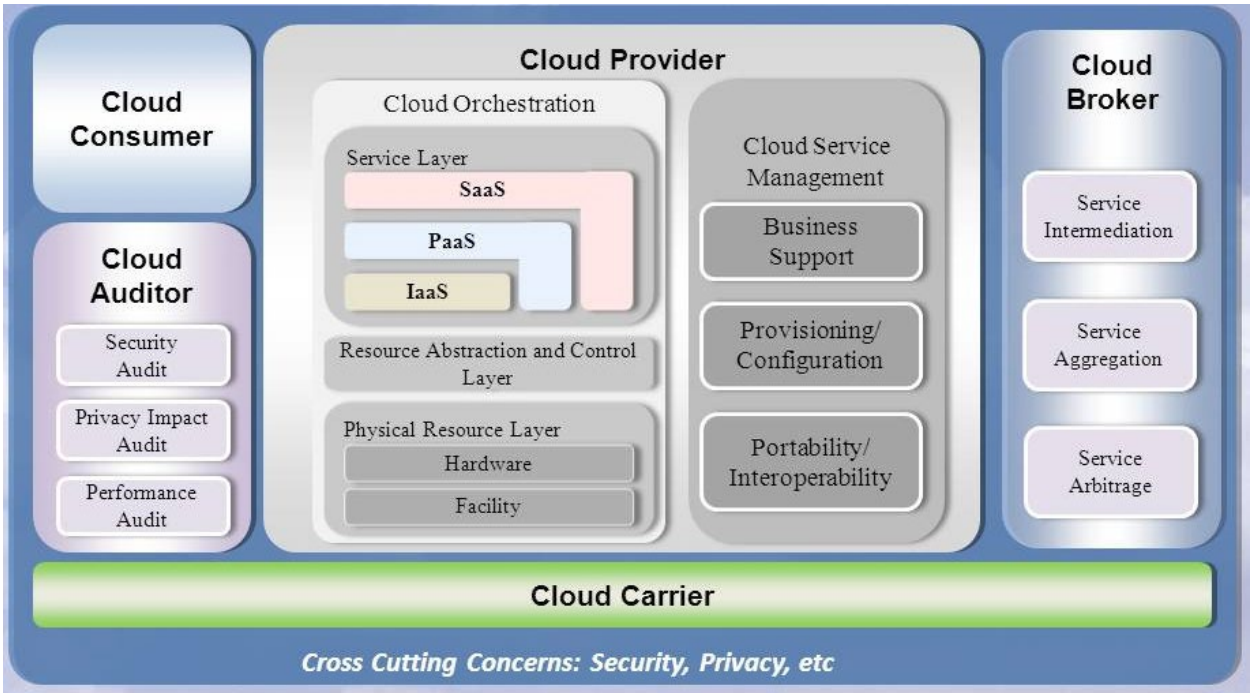
8.6.9. – Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

HRTec provisions physically and logically separated customer areas. As described above, HRTec provides multiple community enclaves within its boundaries. The enclaves are divided by customer vertical State, Local Government & Education (SLED); FedRAMP with two sub enclaves Civilian Federal (CIV), Defense (DEF); and Commercial & Corporate (COM). Within each dedicated enclave tenant separation is ensured based on the deployment model for that tenant. Each enclave is audited monthly for compliance with applicable computer security controls, configurations, vulnerability, and physical access.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

The HRTec Security Technical Reference Architecture generally follows the NIST Security Technical Reference Architecture depicted in **Exhibit 6F: NIST Security Technical Reference Architecture.** HRTec is the Cloud Broker as well as the Cloud Provider. HRTec's Cloud Carrier is accomplished through its Layer 2 Multi-Homing environment and is carrier agnostic. Currently HRTec has engaged two independent Cloud Auditors BlueCanopy and The PMC Group, one for FedRAMP the other for CSA compliance. In addition to this architecture HRTec incorporates the NIST Risk Management Framework (RMF).

Exhibit 6F: NIST Security Technical Reference Architecture



8.6.11. - Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

HRTec Personnel Security Policy & Procedures, HRTec's Facilities Security Program and the National Industry Security Program Operating Manual (NISPOM) establishes the standard procedures and requirements for HRTec personnel who have access to all sensitive data or controlled unclassified information (CUI). Based on what programs the individual will require access to and the role/job/position dictates the extent of the background. HRTec is a Top Secret Cleared facility for the United States Government; with such all employees are US Citizens and minimally a national agency and local agency background check (NACLAC) is conducted.

8.6.12. - Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

As stated above, HRTec's baseline configurations include the use of data encryption for data at rest and data in motion. HRTec's data encryption meet the requirements of FIPS PUB 140-2 Security Requirements for Cryptographic Modules at Security Level 4 and minimally Common Criteria Evaluation Assurance Level EAL4. HRTec integrates additional certificate-based encryption as required by specific contract (e.g. public key infrastructure (PKI)).

8.6.13. - Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

HRTec developed and has implemented an Event/Incident Response Plan (EIRP), its companion HRTec Event/Incident Communication Plan (EICP), and HRTec's Information Spillage Response Standard

Operating Procedure. These plans and procedure provide the framework for stakeholder notifications the plans follow the requirements established by United States Computer Emergency Readiness Team (US-CERT) and the United States Department of Defense (DoD) Defense Industrial Base Cyber Security (DIBCS) Program which currently meet HRTec's FedRAMP High Baseline requirements. HRTec's EIRP and EICP can accommodate any requirements established by a Purchasing Entity. HRTec's EIRP and EICP do include notification of any State-CERT if applicable.

The mitigation of breaches is conducted under HRTec's Information Systems contingency Plan (ISCP), HRTec's Information System Contingency Planning Policy and Procedures and HRTec's Information Spillage Response Standard Operating Procedure. Roles and responsibilities are defined for HRTec staff in the event of a potential breach. If a breach is identified along with the type of breach and what systems are affected HRTec initiates the collection of forensic evidence for analysis. The HRTec ISCP includes notification of HRTec's Insurance carrier, they provide a third-party forensics team to investigate in addition to HRTec's internal team. Law enforcement agencies are notified if necessary, in addition to US-CERT, DIBCS, State-CERT if applicable, and HRTec Legal. Proper notification of other stakeholders (Purchasing Entities, end user, etc.) are conducted per laws and regulations applicable to the specific breach.

6.7. Migration and Redeployment Plan (RFP Section 8.7)

8.7.1. - Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

The HRTec contract manager will work with the Purchasing Entity for an orderly transition for ending contracted services. Paragraph 10 of the SLA describes HRTec's process for this termination and the secure transfer of data.

SLA Para 10. Data Transfer upon Termination or Expiration

10.1 Upon termination or expiration of this Agreement, HRTec will ensure that all [Customer/Agency] and End User Data are securely transferred to the [Customer/Agency], or a Third Party designated by the [Customer/Agency], within thirty (30) calendar days, all as further specified in the technical specifications attached as Exhibit ___. HRTec will ensure that such migration uses facilities and methods that are compatible with the relevant systems of the [Customer/Agency], and that the [Customer/Agency] will have access to the [Customer/Agency] and End User Data during the transition.

10.2 HRTec shall implement its contingency and/or exit plans and take all necessary actions to provide for an effective and efficient transition of service with minimal disruption to the [Customer/Agency]. HRTec will work closely with its successor to ensure a successful transition to the new service and/or equipment, with minimal Downtime and effect on the [Customer/Agency], all such work to be coordinated and performed no less than ninety (90) calendar days in advance of the formal, final transition date.

8.7.2. - Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

The HRTec contract manager will work with the Purchasing Entity for an orderly transfer or return of its data. Paragraph 9 of the SLA describes HRTec's process for this termination and the secure transfer of data.

SLA Para 9. Data Retention and Disposal

9.1. HRTec will retain Data in an End User's account, including attachments, until the End User deletes them or for the time period mutually agreed to by the parties in this Agreement.

9.2. Using appropriate and reliable storage media, HRTec will regularly backup [Customer/Agency] and End User Data and retain such backup copies for a minimum of twelve (12) months.

9.3. At the [Customer/Agency] election, HRTec will either securely destroy or transmit to the [Customer/Agency] repository any backup copies of the [Customer/Agency] and/or End User Data. HRTec will supply the [Customer/Agency] a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.

9.4. HRTec will retain logs associated with End User activity for a minimum of twelve (12) months.

9.5. HRTec will immediately place a "hold" on Data destruction or disposal under its usual records retention policies of records that include the [Customer/Agency] and End User Data, in response to an oral or written request from the [Customer/Agency] indicating that those records may be relevant to litigation that the [Customer/Agency] reasonably anticipates. Oral requests by the [Customer/Agency] for a hold on record destruction will be reduced to writing and supplied to HRTec for its records as soon as reasonably practicable under the circumstances. The [Customer/Agency] will promptly coordinate with HRTec regarding the preservation and disposition of these records. HRTec shall continue to preserve the records until further notice by the [Customer/Agency].

6.8. Service or Data Recovery (RFP Section 8.8)

8.8.1. - Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.

b. Suffers an unrecoverable loss of data.

c. Offeror experiences a system failure.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

HRTec has developed and implemented contingency plans in the event/incident that would disrupt normal operations.

- Extended downtime - generally, if a service goes down HRTec is able to rapidly stand up a new instance for continued service availability in less than 4 hours. HRTec's BDR tool can quickly restore a customer's full or partial system. HRTec operates two geographically separated data centers. If for some reason extended downtime was to occur HRTec can establish operations from the alternate site.
- Suffers an unrecoverable data loss - This would likely not occur as our BDR continually updates (every 5 seconds) the baseline backup and distributes copies locally and to the alternate data center automatically. This action provides the high availability of customer environments. HRTec can restore environments from a full server, application, and data restore; down to a file level restoration; or provide a point in time restoration.
- Offeror experiences a system loss - HRTec's BDR continually updates (every 5 seconds) the baseline backup and distributes copies locally and to the alternate data center automatically. This action provides the high availability of customer environments. HRTec can restore environments from a full system recovery generally within 4 hours.
- Ability to recover and restore data within 4 business hours in the event of a severe system outage - HRTec provides a high availability environment for our customers. We have automatic failover for continuous operations. The automatic failover is nearly instantaneous without loss of data or services.

- Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO) - RPOs for HRTec are customer specific and become part of the SLA at time of contracted services. The maximum RTO for HRTec is 4 hours.

SLA Para 12.1 Interruptions in Service
Notwithstanding the Force Majeure provisions contained herein, HRTec shall be responsible for providing disaster recovery Services if HRTec experiences or suffers a disaster. HRTec shall take all necessary steps to ensure that the [Customer/Agency] shall not be denied access to the Services for more than four (4) Hours in the event there is a disaster impacting any HRTec infrastructure necessary to provide the Cloud Computing Services. HRTec shall maintain the capability to resume provisions of the Services from an alternative location and via an alternative telecommunications route in the event of a disaster that renders HRTec's primary infrastructure unusable or unavailable. If HRTec fails to restore the Services within four (4) Hours of the initial disruption of service, the [Customer/Agency] may declare HRTec to be in default of this Agreement and the [Customer/Agency] may, at their own expense, seek alternate services, which would have otherwise been provided under this Agreement, from Third Parties.

SLA Para 12.2 Service Outage
In the event of a service outage, HRTec will refund or credit the [Customer/Agency], upon [Customer/Agency] election, the pro-rated amount of fees corresponding to the time Services were unavailable.

8.2.2. - Describe your methodologies for the following backup and restore services:
a. Method of data backups
b. Method of server image backups
c. Digital location of backup storage (secondary storage, tape, etc.)
d. Alternate data center strategies for primary data centers within the continental United States.

HRTec utilizes Veeam Availability Suite as its BDR tool. Once baseline images are captured and distributed as described above, they are continually updated for customer systems this would include the entire VM associated with that customer. For HRTec host servers a baseline configuration is established and maintained for all servers. Digital storage locations are local to the primary data center where the customer environment is deployed, and an additional copy is kept and maintained at the alternate data center. For some customers, based on their requirements, an additional encrypted copy is made and provided directly to a customer designated location. For the copy sent to the customer's site the frequency is determined by the customer and is only updated to the point in time of copy made. HRTec's datacenters are located within continental United States.

6.9. Data Protection (RFP Section 8.9)

8.9.1. - Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

As stated above, HRTec's baseline configurations include the use of data encryption for data at rest and data in motion. HRTec's data encryption meet the requirements of FIPS PUB 140-2 Security Requirements for Cryptographic Modules at Security Level 4 and minimally Common Criteria Evaluation Assurance

Level EAL4. HRTec integrates additional certificate-based encryption as required by specific contract (e.g. public key infrastructure (PKI)).

8.9.2. - Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

The HRTec contract manager is responsible for and authorized to sign any applicable Business Associate Agreement or other data protection agreement requested by a Purchasing Entity.

8.9.3. - Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

As stated in paragraph 5 of HRTec's SLA, the use of customer data is limited to specific authorized uses. HRTec monitors the access to all stored data to ensure only authorized users access the data. Purchasing Entities will provide the guidance on data access rights and purposes of use granted to HRTec.

SLA Para 5. Data Privacy

5.1. HRTec will use [Customer/Agency] Data and End User Data only for fulfilling its duties under this Agreement and for the [Customer/Agency]'s and its End User's sole benefit and will not share such Data with or disclose it to any Third Party without the prior written consent of the [Customer/Agency] or as otherwise required by law. By way of illustration and not of limitation, HRTec will not use such Data for HRTec's own benefit and will not engage in "data mining" of [Customer/Agency] or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the [Customer/Agency].

5.2. All [Customer/Agency] and End User Data will be stored on servers located solely within the Continental United States.

5.3. HRTec will provide access to [Customer/Agency] and End User Data only to those HRTec employees, contractors and subcontractors ("HRTec Staff") who need to access the Data to fulfill HRTec's obligations under this Agreement. HRTec will ensure that, prior to being granted access to the Data, HRTec Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

5.4. The [Customer/Agency] shall represents that it is subject to [List all data privacy regulations, laws and policy requirements imposed on the Customer/Agency, it's End Users and Suppliers] (e.g. all applicable federal and state laws restricting the access, use and disclosure of Protected Information and all the terms and conditions contained in Appendix A).

6.10. Service Level Agreement (RFP Section 8.10)

8.10.1. - Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

HRTec's Cloud Computing Service Level Agreement is negotiable. We have provided the requested sample SLA that we use as a baseline for those negotiations as APPENDIX A. Our template has a legend defining the template features that illustrate the areas that are typically negotiated. HRTec is open to negotiation in all areas of the SLA that serve to enhance the quality of the agreement to the mutual benefit of all parties.

HRTec Cloud Computing Solution SLA Legend

Template "Legend":
Highlighted language is variable/changeable information to be entered as appropriate to the specific use case.

Red, italicized text is to provide instructions or other additional information regarding a particular clause. All italicized text should be removed before agreement is executed with any Customer.

RED, CAPITALIZED TEXT IS TO INDICATE THAT AGREEMENT SPECIFIC DATA IS TO BE ENTERED IN PLACE OF THIS TEXT.

8.10.2. - Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

We have provided the requested sample SLA that we use as a baseline for those negotiations as APPENDIX A. This template serves as a baseline for HRTec Cloud Computing Service offerings and is adapted appropriately for the respective service model(s) contracted for by the customer/agency.

6.11. Data Disposal (RFP Section 8.11)

8.11. - Specify your data disposal procedures and policies and destruction confirmation process.

The HRTec ISSO /ISSM acting in conjunction with the customer/agency information system owner:

- Sanitizes all media prior to disposal, release out of organizational control, or release for reuse using techniques and procedures IAW NIST SP 800-88 and our media protection policy and procedures for reuse and disposal of storage media and hardware, and with other applicable federal and contractual standards and policies
- Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Media sanitization will be enforced for all information system media, both digital and non- digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed.

Sanitization techniques employed may include clearing, purging, cryptographic erase, and destruction, to prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Appropriate sanitization methods may require destruction when other methods cannot be applied to media requiring sanitization. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from

a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document.

NOTE: NSA standards and policies control the sanitization process for media containing classified information.

When non-local maintenance services are required from an information system that does not employ compatible security controls the HRTec ISSM ensures the following steps are taken:

- Any component(s) to be serviced are removed or isolated from the information system prior to nonlocal maintenance or diagnostic services
- Organizational information is sanitized for components under service before removal from organizational facilities
- After the service is performed, inspects and sanitizes the component (for potentially malicious software) before reconnecting the component to the information system.

SLA Para 9 Data Retention and Disposal

9.1 HRTec will retain Data in an End User's account, including attachments, until the End User deletes them or for the time period mutually agreed to by the parties in this Agreement.

9.2 Using appropriate and reliable storage media, HRTec will regularly backup [Customer/Agency] and End User Data and retain such backup copies for a minimum of twelve (12) months.

9.3 At the [Customer/Agency] election, HRTec will either securely destroy or transmit to the [Customer/Agency] repository any backup copies of the [Customer/Agency] and/or End User Data. HRTec will supply the [Customer/Agency] a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.

9.4 HRTec will retain logs associated with End User activity for seven (7) years.

9.5 HRTec will immediately place a "hold" on Data destruction or disposal under its usual records retention policies of records that include the [Customer/Agency] and End User Data, in response to an oral or written request from the [Customer/Agency] indicating that those records may be relevant to litigation that the [Customer/Agency] reasonably anticipates. Oral requests by the [Customer/Agency] for a hold on record destruction will be reduced to writing and supplied to HRTec for its records as soon as reasonably practicable under the circumstances. The [Customer/Agency] will promptly coordinate with HRTec regarding the preservation and disposition of these records. HRTec shall continue to preserve the records until further notice by the [Customer/Agency].

6.12. Performance Measures and Reporting (RFP Section 8.12)

8.12.1. - Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

HRTec's reliability and uptime is strong and FedHIVE design considerations for infrastructure and platforms include geographic separation, and redundancy. HRTec operates two data center facilities which are mirrored environments to ensure and guarantee uptime. HRTec utilizes Veeam Availability Suite as its BDR tool for replication, backup, recovery and restoration. Both locations are supported by multiple telecommunication providers, standby emergency generators, and physical security systems.

SLA Para 11. Service Levels

11.1. HRTec represents and warrants that the Cloud Computing Services will be performed in a professional manner consistent with industry standards reasonably applicable to such Services.

11.2. HRTec represents and warrants that the Cloud Computing Services will be operational at least 99.9% of the time in any given month during the term of this Agreement, meaning that the outage or Downtime percentage will be not more than .1%.

11.3. If the Services availability falls below 99.9% in any month, HRTec shall provide the [Customer/Agency] with a credit of that month's bill for Services according to the table below.

AVAILABILITY PERCENTAGE	PERCENTAGE OF CREDIT
99.6% to 99.8%	5%
99.4% to 99.59%	10%
99.0% to 99.39%	15%
97.0% to 98.9%	20%
Below 97.0%	25%

11.4. HRTec represents and warrants that ninety-five percent (95%) of all transactions shall process within no more than one (1) second, and no single transactions shall take longer than five (5) seconds to process.

11.5. If HRTec's system response times fall below the warranted level for two (2) or more consecutive weeks, HRTec shall provide the [Customer/Agency] with a credit in the amount of twenty percent (20%) of the Services fees for that month. If HRTec's system response times fall below the warranted level for six (6) out of eight (8) consecutive weeks, HRTec may be considered to be in default, and the [Customer/Agency] may terminate the Agreement without penalty.

11.6. HRTec shall provide the [Customer/Agency] with any credits resulting from all unachieved service levels in the form of a check provided to the [Customer/Agency] no later than the tenth (10th) business day of the month following the month in which the service levels were not achieved.

11.7. HRTec shall provide the [Customer/Agency] with monthly reports documenting its compliance with the service levels detailed herein. Reports shall include, but not be limited to, providing the following information:
(a) Monthly Services availability by percent time, dates and minutes that Services were not available, and identification of months in which agreed upon service levels were not achieved
(b) Average transaction processing time per week, the fastest and slowest individual transaction processing time per week, the percent of transactions processed that meet the service levels stated herein, and identification of weeks in which agreed upon service levels are not met.

11.8. The [Customer/Agency] may, at its own expense, retain a Third Party to validate HRTec's performance in meeting agreed upon service levels.

8.12.2. - Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

As stated in HRTec's SLA standard uptime is 99.9%. HRTec provides discounts or credit for customers when uptime is not maintained. Uptime does not include HRTec's standard maintenance windows when service is interrupted for patching, system updates and

SLA Para 11. Service Levels

11.1. HRTec represents and warrants that the Cloud Computing Services will be performed in a professional manner consistent with industry standards reasonably applicable to such Services.

11.2. HRTec represents and warrants that the Cloud Computing Services will be operational at least 99.9% of the time in any given month during the term of this Agreement, meaning that the outage or Downtime percentage will be not more than .1%.

11.3. If the Services availability falls below 99.9% in any month, HRTec shall provide the [Customer/Agency] with a credit of that month's bill for Services according to the table below.

AVAILABILITY PERCENTAGE	PERCENTAGE OF CREDIT
99.6% to 99.8%	5%
99.4% to 99.59%	10%
99.0% to 99.39%	15%
97.0% to 98.9%	20%
Below 97.0%	25%

11.4. HRTec represents and warrants that ninety-five percent (95%) of all transactions shall process within no more than one (1) second, and no single transactions shall take longer than five (5) seconds to process.

11.5. If HRTec's system response times fall below the warranted level for two (2) or more consecutive weeks, HRTec shall provide the [Customer/Agency] with a credit in the amount of twenty percent (20%) of the Services fees for that month. If HRTec's system response times fall below the warranted level for six (6) out of eight (8) consecutive weeks, HRTec may be considered to be in default, and the [Customer/Agency] may terminate the Agreement without penalty.

11.6. HRTec shall provide the [Customer/Agency] with any credits resulting from all unachieved service levels in the form of a check provided to the [Customer/Agency] no later than the tenth (10th) business day of the month following the month in which the service levels were not achieved.

11.7. HRTec shall provide the [Customer/Agency] with monthly reports documenting its compliance with the service levels detailed herein. Reports shall include, but not be limited to, providing the following information:
(a) Monthly Services availability by percent time, dates and minutes that Services were not available, and identification of months in which agreed upon service levels were not achieved
(b) Average transaction processing time per week, the fastest and slowest individual transaction processing time per week, the percent of transactions processed that meet the service levels stated herein, and identification of weeks in which agreed upon service levels are not met.

11.8. The [Customer/Agency] may, at its own expense, retain a Third Party to validate HRTec's performance in meeting agreed upon service levels.

8.12.3. - Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

Participating entities have multiple methods for contacting support. Dedicated email, toll free telephone number, and access to HRTec's service ticketing system.

SLA Para 15 Technical Support

15.1 During the term of this Agreement HRTec will provide the [Customer/Agency] and End Users with ongoing technical support for the Cloud Computing Services at no less than the levels and in the manner(s) specified herein.

15.2 HRTec will not withdraw technical support for any Cloud Computing Service without a ninety (90) calendar day advance written notice to the [Customer/Agency], and then only if HRTec is withdrawing technical support from all its customers.

15.3 The [Customer/Agency] acquires the right to use technical support acquired under this Agreement at any location under the direct control of the [Customer/Agency].

15.4 The [Customer/Agency] shall receive at its option the general help desk technical support offered by HRTec to its other customers. Irrespective of HRTec's general technical support offerings, HRTec will provide the [Customer/Agency] with the following technical support:

(a) Answering questions relating to the Cloud Computing Services, including (1) clarification of functions and features of the Services; (2) clarification of the Documentation; (3) guidance in the operation of the Services; and (4) error verification, analysis, and correction, including the failure to produce results in accordance with the Documentation.

(b) Such assistance shall be provided by HRTec twenty-four (24) hours a day, seven (7) days a week via a toll-free telephone number staffed by help desk technicians sufficiently trained and

experienced to identify and resolve most support issues and who shall respond to all [Customer/Agency] requests for support within fifteen (15) minutes after receiving a request for assistance.

(c) HRTec shall provide a current list of persons and telephone numbers for the [Customer/Agency] to contact to enable [Customer/Agency] to escalate its support requests for issues that cannot be resolved by a help desk technician or for circumstances where a help desk technician does not respond within the time specified herein.

(d) In addition to HRTec's obligations under Section 3.2 of this Agreement, HRTec provided telephone technical support shall be compliant with Section 508 of the Rehabilitation Act.

15.5 The following provisions shall be applicable to the correction of Services errors:

(a) If the [Customer/Agency] detects what it considers to be an error in the Cloud Computing Services which causes it not to conform to, or produce results in accordance with, the Documentation, then the [Customer/Agency] shall by telephone or e-mail notify HRTec of the error.

(b) HRTec will deliver to the [Customer/Agency] and keep current a list of persons and telephone numbers (the "HRTec Calling List") for [Customer/Agency] to contact to obtain corrections of Cloud Computing Services errors. The HRTec Calling List shall include: 1) the first person to contact if a question arises or problem occurs; and 2) the persons in successively more responsible or qualified positions to provide the answer or assistance desired. If HRTec does not respond promptly to any request by the [Customer/Agency] for telephone consultative service, The [Customer/Agency] may attempt to contact the next more responsible or qualified person on the HRTec Calling List until contact is made and a designated person responds to the call.

(c) HRTec shall respond within two (2) hours to the [Customer/Agency] initial request for assistance in correcting or creating a workaround for a Cloud Computing Services error. HRTec's response shall include assigning fully-qualified technicians to work with the [Customer/Agency] to diagnose and correct or create a workaround for the Cloud Computing Services error and notifying the [Customer/Agency] representative making the initial request for assistance of HRTec's efforts, plans for resolution of the error, and estimated time required to resolve the error.

(d) For Class 1 Errors, within twenty-four (24) hours after the [Customer/Agency] first reports the error, HRTec will provide a correction or workaround acceptable to the [Customer/Agency]. HRTec's correction process will include assigning fully-qualified technicians to work with the [Customer/Agency] without interruption or additional charge.

(e) If HRTec fails to provide a reasonable correction or workaround for a Class 1 Error within twenty-four (24) hours, HRTec shall provide a price adjustment reflecting the reduction of value the [Customer/Agency] will incur as a result of the Class 1 Error and not as a penalty or compensation for damage, the sum of 1/365 of the technical support fees, expressed as an annual charge, for each additional day or part thereof that HRTec fails to provide a reasonable correction or workaround for the Class 1 Error. HRTec will provide such payment in the form of a check provided to the [Customer/Agency] no later than the tenth (10th) business day following the month in which failure to correct occurred.

(f) The Project Managers, or such persons as otherwise designated by the [Customer/Agency] and HRTec, shall serve as said parties' contacts for all communications relating to technical support. Each party may change its own contact person by written notice to the other party.

15.6 The following provisions shall set forth HRTec's obligations to provide Enhancements:

- HRTec will generally enhance and improve the Cloud Computing Services for as long as the [Customer/Agency] elects to receive and pays for the Cloud Computing Services.
- HRTec will provide to the [Customer/Agency] during the Agreement term, (1) all Enhancements which it develops with respect to the Cloud Computing Services; (2) any and all Enhancements required by federal or state governmental, or professional regulatory mandates related to [Customer/Agency] use of the Cloud Computing Services; and (3) the Documentation associated with any Enhancements.
- HRTec will provide Enhancements to the [Customer/Agency] upon their general release and no later than the time when the first five percent (5%) of HRTec's customers receive those Enhancements.

- Except as otherwise provided in a signed addendum to this Agreement, nothing herein shall obligate HRTec to enhance the Cloud Computing Services in any respect or on any particular date. The decision as to whether and/or when, to enhance the Cloud Computing Services will be within HRTec's discretion.

15.7 HRTec will provide the [Customer/Agency] with sixty (60) calendar days advance written notice of proposed product changes as well as product road maps relating to the Cloud Computing Services provided to the [Customer/Agency] under this Agreement.

8.12.4. - Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

If there was although highly unlikely that HRTec's CERT would fail to respond to an incident or fail to take corrective action within the timeframes there are two areas that provide remedies for Customers within the SLA. Please refer to the following exerts from the SLA for details.

SLA Para 23.2. Services Warranty. HRTec represents and warrants that the Cloud Computing Services provided to the [Customer/Agency] under this Agreement shall conform to, be performed, function, and produce results substantially in accordance with the Documentation. HRTec offers the [Customer/Agency] warranty coverage equal to or greater than that offered by HRTec to any of its customers. HRTec's obligations for breach of the Services Warranty shall be limited to using its best efforts, at its own expense, to correct or replace that portion of the Cloud Computing Services which fails to conform to such warranty, and, if HRTec is unable to correct any breach in the Services Warranty by the date which is ninety (90) calendar days after the [Customer/Agency] provides notice of such breach, the [Customer/Agency] may, in its sole discretion, either extend the time for HRTec to cure the breach or terminate this Agreement.

8.12.5. - Describe the firm's procedures and schedules for any planned downtime.

HRTec has regularly scheduled non-emergency maintenance periods typically conducted over the last weekend of the month. As stated in the below exert of the SLA, a reminder notice will be sent with the date and times.

SLA Para 12.5 HRTec will provide the [Customer/Agency] with a reminder notice five (5) calendar days prior with the times that the Cloud Computing Services will be unavailable due to non-emergency maintenance or Enhancements. HRTec will schedule any such times (i.e. planned maintenance) that the Services will be unavailable during the last weekend of every month generally between the hours of 11:00 pm Eastern Time and 5:00 am Eastern Time. In the event of unscheduled and unforeseen times that the Cloud Computing Services will not be available for any reason, except as otherwise prohibited by law, HRTec will immediately notify the [Customer/Agency] and cooperate with reasonable requests for information regarding the Services being unavailable (including causes, effect on Services, and estimated duration).

8.12.6. - Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Should HRTec's BDR process fail to restore or recover within the timeframes there are two areas that provide remedies for Customers within the SLA. Please refer to the following exerts from the SLA for details.

SLA Para 23.2. Services Warranty. HRTec represents and warrants that the Cloud Computing Services provided to the [Customer/Agency] under this Agreement shall conform to, be performed, function, and produce results substantially in accordance with the Documentation. HRTec offers the [Customer/Agency] warranty coverage equal to or greater than that offered by HRTec to any of its customers. HRTec's obligations for breach of the Services Warranty shall be limited to using its best efforts, at its own expense, to correct or replace that portion of the Cloud Computing Services which fails to conform to such warranty, and, if HRTec is unable to correct any breach in the Services Warranty by the date which is ninety (90) calendar days after the [Customer/Agency] provides notice of such breach, the [Customer/Agency] may, in its sole discretion, either extend the time for HRTec to cure the breach or terminate this Agreement.

8.12.7. - Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

Performance reports are available over the Web and can be downloaded or printed from the customer/agency admin portal. These reports are typically provided based on user role. Performance reports currently are point-in-time statistics that are collected on an agreed upon schedule (i.e. every Friday after 1200 eastern, monthly at close of business the 10th day of each month, daily at 1500 pacific, etc.). Performance report schedules are currently driven by customer/agency requirements and negotiated in the contracting process. HRTec is in work on the development of a dashboarding system that can be used for customer/agency personnel to visualize and/or download/print real-time performance statistics from their admin portal.

8.12.8. - Ability to print historical, statistical, and usage reports locally.

Historical, Statistical, and Usage reports are available in the customer/agency admin portal. These reports are typically provided based on user role. All customer/agency specific reports are archived throughout the lifecycle of service and available for download/print from the customer/agency admin portal.

8.12.9. - Offeror must describe whether or not its on-demand deployment is supported 24x365.

HRTec's on demand deployment is available 24x365; except for during service maintenance times. This service is restricted to existing customer deployed environments and pre-authorized customers.

8.12.10. - Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

HRTec's on demand deployment is available 24x365; with the exception of service maintenance times. This service is restricted to existing customer deployed environments and pre-authorized customers.

6.13. Cloud Security Alliance (RFP Section 8.13)

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.
a. Completion of a CSA STAR Self-Assessment. (3 points)
b. Completion of Exhibits 1 **and** 2 to Attachment B. (3 points)
c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
d. Completion CSA STAR Continuous Monitoring. (5 points)

In response to this requirement and in the interest of providing transparency of our security practices as a cloud services provider, HRTec has registered with the Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) to document the security controls provided by our various cloud computing

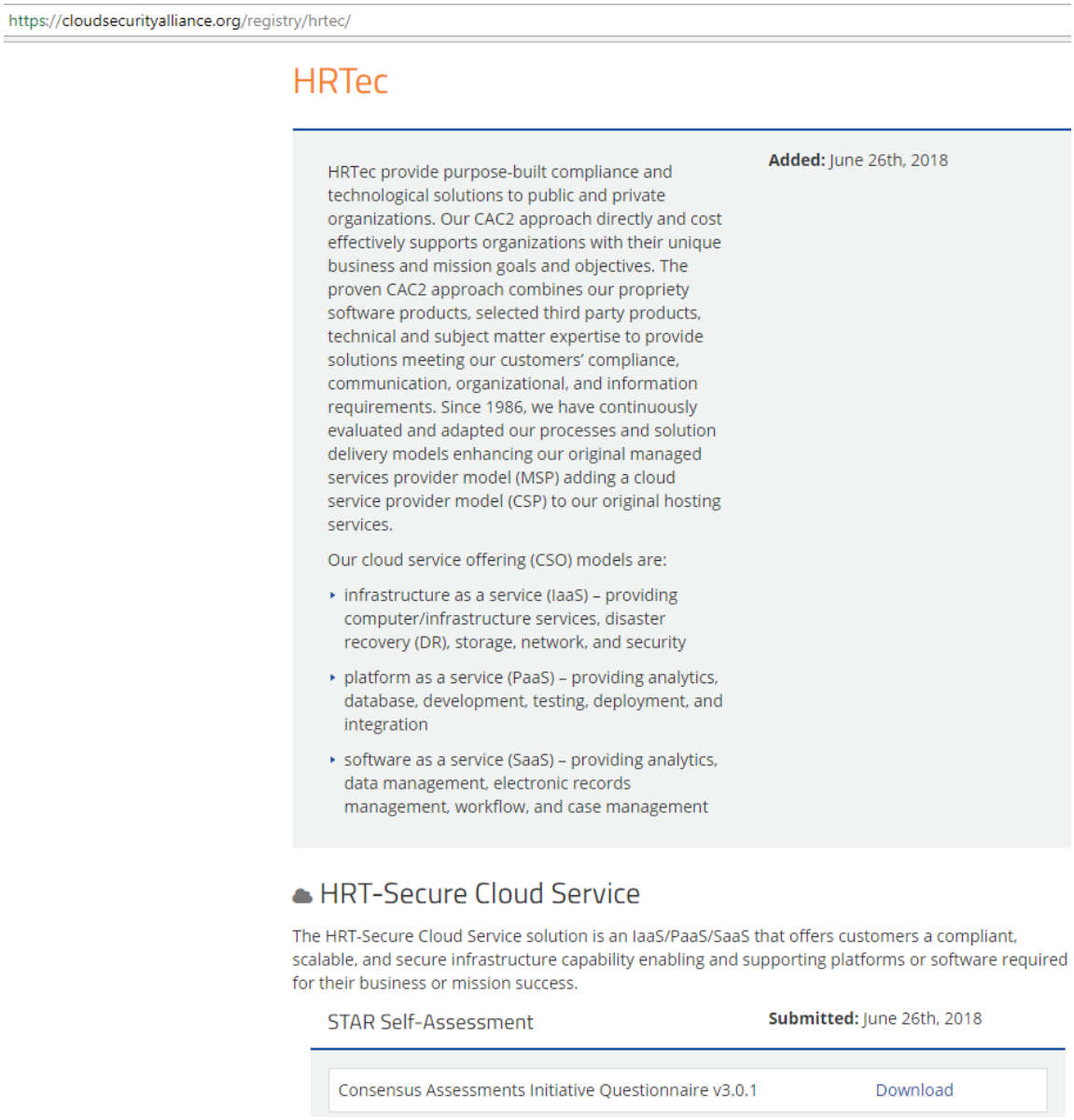
offerings to aid users and potential users as they assess the security of our cloud offerings that they are or may contract for. HRTec has completed the CSA Consensus Assessments Initiative Questionnaire (CAIQ). This CAIQ published by the CSA provides a way to reference and document what security controls exist in HRTec's IaaS, PaaS, and SaaS Service offerings. The CAIQ provides 295 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. The CAIQ also cross-references the questions with over 25 international security standards, assessments, accreditations and initiatives.

HRTec is listed in the CSA Star registry at: https://cloudsecurityailliance.org/registry/hrtec .

- Completion of a CSA STAR Self-Assessment. (3 points)
  - HRTec has completed its Self-Assessment as evidenced by our CSA registration and the separately attached completed Exhibits.
- Completion of Exhibits 1 **and** 2 to Attachment B. (3 points)
  - HRTec has completed Exhibits 1 and 2 to Attachment B and those exhibits have been provided as supplier attachments to this proposal.
- Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)

HRTec has engaged The PMC Group, LLC to perform Attestation, Certification and Assessment of HRTec's CSA STAR Self-Assessment and anticipate completion of this assessment prior to August 1, 2018.

Exhibit 6G: HRTec CSA STAR Registry



- Completion CSA STAR Continuous Monitoring. (5 points)

Since the CSA STAR Continuous Monitoring requirements are currently under development, HRTec is providing **Exhibit 6H: FedHIVE Continuous Monitoring Plan** to demonstrate our employed continuous monitoring practices. We are confident that our continuous monitoring practices in support of our FedRAMP High Baseline align with the CSA STAR Continuous Monitoring guidelines once published.

Exhibit 6H: FedHIVE Continuous Monitoring Plan

FedRAMP Continuous Monitoring Plan							
CSP:	**HRTec**		**Original ATO Date:**		**Last Updated:**	**6/30/2017**	
CSO:	**Federal High Impact Virtualized Environment**		**Completed by:**	**Brian VdM**	**Agency if applicable:**		
Impact Level:	**High**		**Service Model:**	**Iaas, PaaS & SaaS**	**Deployment Model:**	**Community**	
No.	**Control Name**	**Control ID**	**Description**	**Frequency**	**Responsible**	**Deliverable**	**Evidence/Artifact**
1	Information System Monitoring	SI-4	Monitors the system in accordance with SI-4 control requirements.	Continuous/ Ongoing	CSP	Evidence	Manual and Automated Tools
2	Auditable Events	AU-2d	Monitor required events	Continuous/ Ongoing	CSP	Evidence	Monitor required events
3	Information System Component Inventory	CM-8(3)a	Automated detection of new assets	Continuous/ Ongoing	CSP	Evidence	SEIM
4a	Incident Reporting	IR-6	Incident reporting and tracking	Continuous/ Ongoing	CSP	Evidence	Manual and Automated Tools
4b	Incident Reporting	IR-6	Incident reporting and tracking	As Required	CSP	Report	Manual and Automated Tools
5	Temperature & Humidity Controls	PE-14(b)	Monitor	Continuous/ Ongoing	CSP	Evidence	Facility Mgmt
6	Vulnerability Scanning	RA-5(2)	Update list of vulnerabilities scanned before each scan	Continuous/ Ongoing	CSP	Evidence	SEIM
7	Wireless Intrusion Detection	SI-4(14)	Monitors for unauthorized wireless connection points	Continuous/ Ongoing	CSP	Evidence	Manual and Automated Tools
8	Contingency Planning	CP-3(a)	Evidence	10 Days	CSP	Evidence	NIH & DoD Certificates
9	Audit Review, Analysis, & Reporting	Au-6a	Review/analyze audit records and report findings of anomalies	Weekly	CSP	Evidence	Security Audit Folders
10	Vulnerability Scanning	RA-5d	Provide artifacts to ISSO showing high-risk vulnerabilities have been mitigated in 30 days and moderate risk-vulnerabilities within 90 days	Monthly	CSP	Report	POAM
11	Continuous Monitoring Security State	CA-7g	Report security state of the system to own organization	Monthly	CSP	Evidence	Monthly Security Audit report
12	Access Records	PE-8b	Review visitor access records	Monthly	CSP	Evidence	PACS Access Logs and Visitor Sign-in Sheet
13	Least Functionality	CM-7(1)a	Identify and eliminate unnecessary functions, ports, protocols, and/or services	Monthly	CSP	Evidence	SEIM

No.	Control Name	Control ID	Description	Frequency	Responsible	Deliverable	Evidence/Artifact
14	Vulnerability Scanning	RA-5a	OS/infrastructure/ web application/ database scans	Monthly	CSP	Report	SCAP/SEIM
15	Flaw Remediation	SI-2c	Install security-relevant software and firmware updates within 30 days of the release of the updates.	Monthly	CSP	Evidence	SEIM/Web ROOT
16	Flaw Remediation	SI-2(2)	Automated look for system flaws	Monthly	CSP	Evidence	SEIM/Web ROOT
17	Software & Information Integrity	SI-7(1)	Perform integrity scans	Monthly	CSP	Evidence	SEIM/Web ROOT
18	Account Management	AC-2(2)	Automatic termination of temporary and emergency accounts after no more than 30 days. Automatic termination of temporary and emergency accounts after no more than 30 days	Monthly	CSP	Evidence	Manual Disable and Delete and Recorded in Audit Trail
19	Security Functionality Verification	SI-6	Verify correct operation of security functions	Monthly	CSP	Evidence	SEIM/Web ROOT
20	Plan of Action & Milestones	CA-5	Update as monthly and submit to ISSO	Monthly	CSP	Report	POAM
21	Monitoring Physical Access	PE-6b	Review physical access logs and record date in SSP	Monthly	CSP	Evidence	Facility Mgmt
22	Authenticator Management	IA-5g	Change/refresh authenticators at least every sixty days	60 Days	CSP	Evidence	AD
23	Account Management	AC-2(3)	Disable user IDs after 90 days inactivity	90 Days	CSP	Evidence	Manual Disable and Delete and Recorded in Audit Trail
24	Identifier Management	IA-4e	Disables user IDs after 90 days of inactivity.	90 Days	CSP	Evidence	Manual Disable and Delete and Recorded in Audit Trail
25	Publicly Accessible Content	AC-22d	Review content on publicly accessible system and look for non-public information.	90 Days	CSP	Evidence	Monthly Security Audit report
26	Access Restrictions for Change	CM-5(5)b	Review and reevaluate their information system developer/integrator privileges quarterly.	90 Days	CSP	Evidence	Monthly Security Audit report
27	Information Security Policies	All "-1" Controls	Review and update	Annually	CSP	Evidence	Annual Document Updates
28	Account Management	AC-2j	Review and re-certify user accounts and record date in SSP	Annually	CSP	Evidence	Monthly Security Audit report

No.	Control Name	Control ID	Description	Frequency	Responsible	Deliverable	Evidence/Artifact
29	Security Awareness	AT-2	Provide basic security awareness training and record date in SSP	Annually	CSP	Evidence	NIH & DoD Certificates
30	Auditable Events	AU-2(3)	Review and update auditable events and record changes and date in SSP	Annually	CSP	Evidence	Monthly Security Audit report
31	Security Assessments	CA-2b	Assess subset of security controls	Annually	3PAO	Report	3PAO Report
32	Security Assessments	CA-2	Plan for the annual assessment and conduct the assessment	Annually	3PAO	Report	3PAO Report
33	Security Assessments - Specialized Assessments	CA-2(20	Testing in accordance with FedRAMP specific requirements as part of annual assessment	Annually	3PAO	Report	3PAO Report
34a	Penetration Testing	CA-8, CA-8 (1)	CSP at least annually and as needed and 3PAO penetration testing as part of annual assessment	Annually	CSP	Report	HRTec Annual PEN Test Report
34b	Penetration Testing	CA-8, CA-8 (1)	CSP at least annually and as needed and 3PAO penetration testing as part of annual assessment	Annually	3PAO	Report	3PAO Report
35	Baseline Configuration and System Component Inventory	CM-2(1)a	Reviews and update baseline configuration annually or during installations and updates	Annually	CSP	Evidence	Annual Document Updates
36	Configuration Management Plan	CM-9	Review and update	Annually	CSP	Evidence	Annual Document Updates
37	IT Contingency Plan	CP-2d	Review and update	Annually	CSP	Evidence	Annual Document Updates
38	IT Contingency Training	CP-3	Train personnel in contingency roles and responsibilities and record date in SSP	Annually	CSP	Evidence	Quartely ISCP Tabletop
39	IT Contingency Plan Testing & Exercises (Moderate Systems)	CP-4a	Test and exercise IT Contingency Plan - Insert into Appendix F of IT Contingency Plan	Annually	CSP	Report	Quartely ISCP Tabletop
40	Information System Backup	CP-9(1)	Test backups to verify integrity and reliability and record date in SSP	Annually	CSP	Evidence	Quartely ISCP Tabletop
41	Incident Response Training	IR-2c	Conduct incident response training and record date, training materials and participants in SSP	Annually	CSP	Evidence	Semi Annual EIRP Training

No.	Control Name	Control ID	Description	Frequency	Responsible	Deliverable	Evidence/Artifact
42	Incident Response Testing	IR-3	Perform incident response testing -and date, results, and participants in SSP	Annually	CSP	Report	Semi Annual EIRP Training
43	Incident Response Plan	IR-8	Review and update	Annually	CSP	Evidence	Semi Annual EIRP Training
44	Physical Access Authorizations	PE-2c	Review physical access authorization credential and record date and who performed it in SSP	Annually	CSP	Evidence	Facility Mgmt
45	Physical Access Control	PE-3f	Inventory physical access devices annually and record date in SSP	Annually	CSP	Evidence	Facility Mgmt
46	Physical Access Control	PE-3g	Change combinations and keys annually and record date and name of responsible person in SSP	Annually	CSP	Evidence	Facility Mgmt
47	System Security Plan	PL-2c	Review and update	Annually	CSP	Evidence	Annual Document Updates
48	Access Agreements	PS-6b, PS-6c	Review and update and record date in SSP	Annually	CSP	Evidence	Annual Document Updates
49	Vulnerability Scan	RA-5a	Scan OS/infrastructure, web applications, and databases	Annually	3PAO	Report	3PAO Report
50	Boundary Protection	SC-7(4)e	Remove traffic flow that is no longer supported by business/mission need	Annually	CSP	Evidence	Manual and Automated Tools
51	Security Training	AT-3b, AT-3c	Annual role-based training	Annually	CSP	Evidence	NIH & DoD Certificates
52	Security Awareness Training Records	AT-4b	Archive training records	Annually	CSP	Evidence	Human Resources
53	Identifier Management	IA-4d	Prevent reuse of user and device identifiers every 2 years	Every Two Years	CSP	Evidence	Manual and Automated Tools
54	Security Authorization	CA-6c	Record date of any reauthorization in SSP	Every Three Years	CSP	Evidence	Annual Document Updates
55	IT Contingency Plan Testing & Exercises (Low Systems)	CP-4a	Test and exercise the IT Contingency Plan	Every Three Years	CSP	Report	Quartely ISCP Tabletop
56	Position Categorization	PS-2c	Review position categorizations and record date in SSP	Every Three Years	CSP	Evidence	HRTes Policies & Procedures

No.	Control Name	Control ID	Description	Frequency	Responsible	Deliverable	Evidence/Artifact
57	Risk Assessment	RA-3c, e	Review and update security assessments and record date in SSP	Every Three Years	CSP	Evidence	HRTec Corporate Risk Mgmt Plan
58	Personnel Screening	PS-3b	Law enforcement must undergo personnel screening every 5 years - record date and names in SSP	Every Five Years	CSP	Evidence	NAC/LAC

6.14. Service Provisioning (RFP Section 8.14)

8.14.1 - Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

HRTec will process emergency or rush requests from Purchasing Entities in a similar process as a normal request. The deployment will operate through our TDE until we are able to ensure the requested implementation meets our production environment's security and functionality requirements. A normal request for access to the new implementation only provide for access in a restricted mode. The emergency or rush implementation would not have the access restriction and would mimic a full deployment into the production environment. Upon successful completion of testing and at a time acceptable to the Purchasing Entity the emergency or rush environment would be transferred to the production environment for continued full deployment and access.

8.14.2 - Describe in detail the standard lead-time for provisioning your Solutions.

Lead-time for initial provisioning of an IaaS or PaaS environment is within 2 hours to ensure all security controls are in place and fully functional. HRTec's SaaS services are based on the extent of customization requested by the Customer. Upon competition of the customization and final testing for security controls, the SaaS service can be provisioned in less than 2 hours.

6.15. Back Up and Disaster Plan (RFP Section 8.15)

8.15.1 - Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

HRTec is well versed with and has in place the ability and capability of applying all legal retention and disposition requirements specific to any Purchasing entity. HRTec currently supports and provides retention services to a diverse set of entities from the Department of Defense to nonprofit organizations.

8.15.2 - Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Currently HRTec is not aware of any inherent disaster recovery risks. All plans and procedures supporting disaster recovery are exercised at least annually. Additionally, testing of backups and the ability recover and restore is accomplished quarterly.

8.15.3 - Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

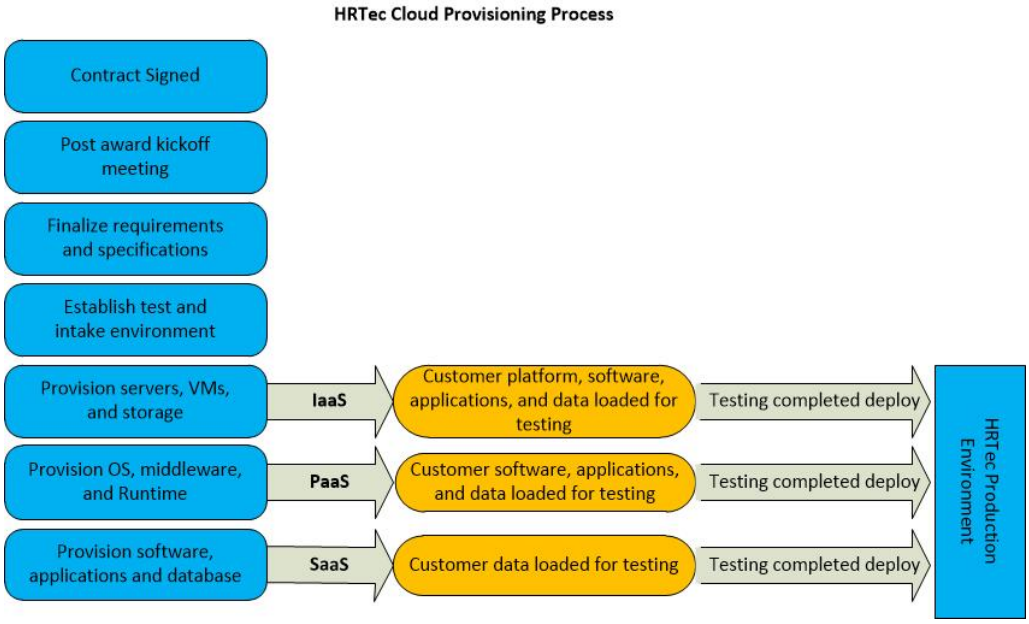
HRTec operates a mirrored environment at both data centers. They are connected via encrypted secure VPNs operating Secure VLANs for management and operational readiness. The sites operate under a High Availability model with layer 2 multihoming BGP routers. Multiple geographically separated telecommunication circuits service both facilities. Either site can be a primary both with premise-based management and security tools. HRTec personnel are available to respond to both facilities. Large scale applications are currently operating, supported, mirrored, and supporting approximately 1.8 million end users.

6.16. Hosting and Provisioning (RFP Section 8.16)

8.16.1 - Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

HRTec's cloud provisioning process varies slightly with the service offering requested as illustrated in **Exhibit 6I: HRTec Cloud Provisioning Process**.

Exhibit 6I: HRTec Cloud Provisioning Process



8.16.2 - Provide tool sets at minimum for:
1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)
2. Creating and storing server images for future multiple deployments
3. Securing additional storage space
4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

HRTec provided tools sets support:

- HRTec's standard server deployment whether as a new standalone or augmenting an existing server farm are deployed and configured to our baseline configuration which is imaged by our Veeam Availability Suite. The image is validated utilizing our SCAP tool
- Server images are created by the Veeam Availability Suite, images are stored at both datacenters.
- Additional storage space is managed through MS System Center's deployment tool.
- HRTec's SOC will provide access to performance reports and are available on the customer/agency admin portal. These reports are typically provided based on user role. Performance reports currently are point-in-time statistics that are collected on an agreed upon schedule (i.e. every Friday after 1200 eastern, monthly at close of business the 10th day of each month, daily at 1500 pacific, etc.). Performance report schedules are currently driven by customer/agency requirements and negotiated in the contracting process. HRTec is in work on the development of a dashboarding system that can be used for customer/agency personnel to visualize and/or download/print real-time performance statistics from their admin portal.

6.17. Trial and Testing Periods (Pre and Post Purchase) (RFP Section 8.17)

8.17.1 - Describe your testing and training periods that your offer for your service offerings.

HRTec's Test and Development Environment (TDE) for verification and validation (V&V) of the requested changes, patches and new implementations is available the same periods as the production environment. The TDE is a standalone enclave which mimics the production environment. The testing environment is segregated physically from the development environment. HRTec's testing processes are required in support of or FedRAMP High Baseline compliance.

HRTec training is available online with its associated SaaS products. Any instructor led training would be scheduled when appropriate. Instructor led training has been conducted days, nights, and weekends on or offsite. Training expectations are defined at the time of award and documented within the SLA.

SLA Para 16. Training

16.1. HRTec will provide the [Customer/Agency] with training for the purposes of understanding and using the Cloud Computing Services ("Training Services"). Training Services will be provided by HRTec as detailed below at no additional cost to the [Customer/Agency]. Training Services will be provided by HRTec to the [Customer/Agency] at mutually agreeable dates and times, but no later than one hundred eighty (180) calendar days following the Effective Date of this Agreement.

16.2. [INCLUDE DESCRIPTION, FREQUENCY AND TIMING OF ANY NEGOTIATED TRAINING SERVICES HERE (OR AS A REFERENCED ATTACHED SCHEDULE)].

8.17.2 - Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

HRTec's production environment has been operational for some time supporting multiple customer approved implementations. Any test or proof of concept is conducted through HRTec's TDE. HRTec would provide the customer with non-public access for these purposes. For HRTec SaaS offerings, a limited functionality demo is available and accessible for customer evaluation. The limited functionality is primarily no output capabilities. If the customer has issued a contract to HRTec, a full function environment is stood up in the TDE for customer access through the customization of the SaaS offering. This allows

customers to test, review, and approve the customization prior to transfer into the production environment. Any test data within the system is removed prior to production.

8.17.3 - Offeror must describe what training and support it provides at no additional cost.

HRTec's SaaS offerings come with a self-help module for training at no additional cost. This training module has complete information on the offering that can be accessed anytime.

6.18. Integration and Customization (RFP Section 8.18)

8.18.1 - Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

As part of the customization phase, HRTec's DevOps team will provide support and integration of APIs for system interconnection. These interconnections will be completely documented and tested for functionality and security. These steps are taken to ensure both system retain integrity, poise no threat to other tenant environments, and poise no threat to the integrity and security of HRTec's production environments and infrastructure.

8.18.2 - Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

HRTec service offerings IaaS PaaS and SaaS are customizable based on a Purchasing Entity's requirements. HRTec's Program Manager and DevOps Team will meet with the Purchasing Entity's Team and finalize all customization requirements and business cases. A project schedule will be formalized and along with the completed requirements and business cases for the Purchasing Entity to approve. Once approved the customization will begin. The HRTec Program Manager will provide weekly status reports and schedule team meetings with the Purchasing Entity as needed. As described above the Purchasing Entity will have access to the TDE for testing and funal approval of the customizations.

6.19. Marketing Plan (RFP Section 8.19)

8.18.1 - Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Initially and without delay after MSA award we will ensure that we complete the steps for providing ordering instructions for inclusion in the NASPO ValuePoint eMarket Center as identified in the RFP. We will add product information and ordering instructions to our offerings on our website specifically supporting ValuePoint participants. Moreover, HRTec understands that unlike the IBMs and AT&Ts of the world we cannot rely on name recognition alone to promote our cloud computing solutions, so we employ a practical five step process for outreach marketing of our cloud services to governmental customers and agencies.

1. Research and identify prime prospects at participating states and purchasing entities for the cloud services within our line of business to determine which groups need which types of services. For example, IaaS/PaaS solutions will be of interest to PCOs and CIOs, our SaaS offerings to EEO and Title IX process owners, etc.

2. Clearly identify the attributes that differentiate our offerings. Examples include affordability, compliance, security, performance, availability, support, and bundling.
3. Create a Communications Plan that defines what information will be communicated, how it will be communicated, and when it will be distributed to which audience. The plan will identify the organizations, events, social media and other channels that influence the targeted prospects.
4. Plan for and conduct public relations activities (press releases, blogs, events attendance and displays or booths, and other methods to market our solutions and expertise to participating states and purchasing entities.
5. Develop tailored marketing campaigns that address specific needs of each customer group that includes education, showcases use cases and other methods of building rapport within the target community of prospects.

Additionally, HRTec agrees to cooperatively engage with NASPO ValuePoint personnel per the Cooperative Program Marketing and training requirements defined in paragraph 43 of the MSA.

6.20. Related Value-Added Services to Cloud Solutions (RFP Section 8.20)

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

HRTec offers a full range of professional and managed services. **Exhibit 6J: HRTec Value-Added Services** lists additional HRTec services available to assist Purchasing Entities with service and support requirements. These Services may be acquired as Time and Materials or Firm Fixed Price.

Exhibit 6J: HRTec Value-Added Services

HRTec Capabilities & Services	
Full-service IT support	Custom web-based applications
Web site design, development and hosting	Graphic design
Software design and development	Cloud-based e-mail
Network engineering	Help desk applications & support
Organizational & employee climate assessments	Global, secure telecommunications networks
Specialized research and reports	Needs assessments

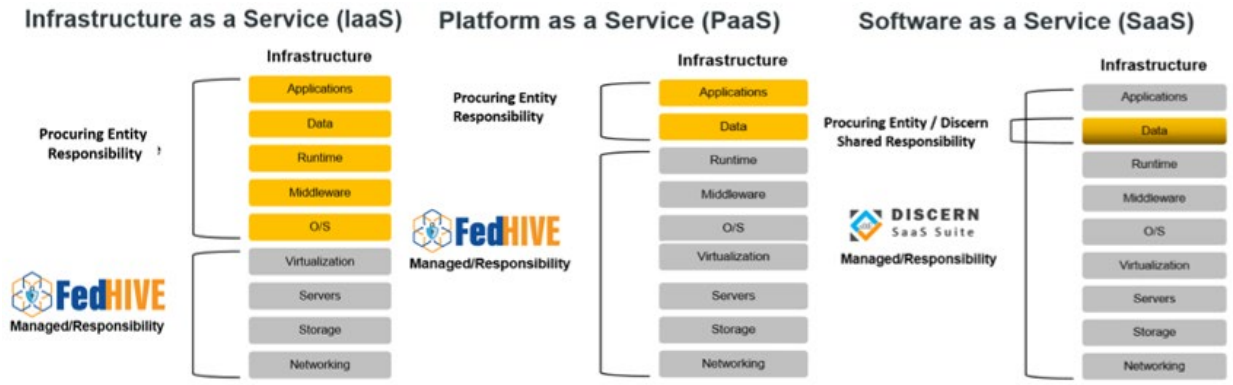
6.21. N/A (RFP Section 8.21)

6.22. Supporting Infrastructure (RFP Section 8.22)

8.22.1 - Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

As a full stack Cloud Services Provider HRTec provides the appropriate deployment service model infrastructure as illustrated in **Exhibit 6K: Supporting Infrastructure**. The procuring entity will be responsible for the systems/layers of the infrastructure as shown, dependent on contracted services deployment model.

Exhibit 6K: Supporting Infrastructure



8.22.2 - If required, who will be responsible for installation of new infrastructure and who will incur those costs?

HRTec assumes all responsibility for the installation of new infrastructure as illustrated in **Exhibit 6K: Supporting Infrastructure** and will incur all costs associated with the installation of the new infrastructure. The procuring entity will be responsible for providing the deployment services model systems/layers identified as procuring entity responsibility in the exhibit. The HRTec ISWF will perform the installation following our change management policies and procedures which include installation of an initial instantiation within our TDE for test and verification prior to transfer to the production environment for formal deployment. HRTec will incur the installation labor costs.

Cloud Computing Service Agreement for NASPO ValuePoint Infrastructure and/or Platform Customers

1. **Scope**

   This agreement applies to any service or combination of services ordered by the Participating Entity and provided by HRTec to customer that involves the provision of FedHIVE Infrastructure and or Platform services to host applications and data used by the Participating Entity (collectively, "the service"). The types of services include but are not limited to:

Service Model	Service Model Subcategory	Data Risk Category	Deployment Model
IaaS	Computer/Infrastructure Services, Disaster Recovery, Storage, Network, Security	Low, Moderate, & High	Private, Community, Hybrid
PaaS	Analytics, Database, Development, Testing and Deployment, Integration, Open Source	Low, Moderate, & High	Private, Community, Hybrid

2. **Modifications to this Agreement**

   This Service Agreement is designed to be supplemental to the NASPO ValuePoint Master Service Agreement and Exhibits 2 and 3 thereof. This Service Agreement may be revised to incorporate changes, additions, and /or deletions resulting from Participating Entity negotiations for inclusion/exclusion in an executed Participating Addendum.

3. **Termination**

   Participating Entities may terminate this Service Agreement per the terms of the NASPO Master Agreement paragraph 7 and the executed Participating Addendum. HRTec shall provide for data preservation and/or disposition per paragraph 7 of the Exhibits 2 and 3, unless specified otherwise in the executed Participating Agreement.

4. **Term, Billing Cycle, and Renewal Term**

   The term, billing cycle, and renewal term of this Service Agreement shall be specified in the executed Participating Addendum.

5. **Access and Use**

   Subject to the terms and conditions contained in this Agreement, HRTec agrees to provide the features and functions of FedHIVE Cloud Computing Services in connection with one or more Participating Entity Applications (as identified in an applicable Participating Addendum Exhibit) during the Participating Addendum Term, solely for use by the Participating Entity, its Authorized Entity(ies) and its End Users, solely in accordance with any documentation provided by HRTec. The Participating Entity acknowledges and agrees that, as between the Participating Entity and HRTec, the Participating Entity shall be responsible for all acts and omissions of Authorized Entities, and any act or omission by an Authorized Entity which, if

undertaken by the Participating Entity, would constitute a breach of this Addendum, shall be deemed a breach of this Addendum by the Participating Entity.

6. **Disclaimer of Warranties/Limitation of Liability**

Except as explicitly provided for in the NASPO Master Agreement, Exhibits 2 and 3 thereof, and the Participating Addendum, HRTec hereby expressly disclaims all warranties of any nature, express, implied or otherwise, including but not limited to any implied warranties of merchantability, noninfringement, or fitness for a particular purpose. HRTec does not guarantee or warranty the deliverability of any data generated by, hosted by or otherwise passed through HRTec owned or operated equipment or computer systems. The Participating Entity expressly agrees that HRTec shall not be liable for damages of any kind which arise directly or indirectly out of the non-delivery of data generated by, hosted by or otherwise passed through HRTec owned or operated equipment or computer systems.

HRTec is a distributor and not a publisher of the content supplied by customer; as such, HRTec exercises no editorial control over such content. The Participating Entity agrees to indemnify, defend and hold HRTec and its affiliates, partners and licensors and each of their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses arising out of or in connection with any claim arising out of (a) Participating Entity use of the service in a manner not authorized by this agreement, and/or in violation of the applicable restrictions, acceptable use policy, and/or applicable law and (b) Participating Entity or Participating Entity employees or representatives negligence or willful misconduct.

Participating Entity expressly agrees that HRTec shall not be liable for damages of any kind, including but not limited to special, incidental, and/or consequential damages (including, without limitation, costs of procuring substitute products or services) which arise directly or indirectly out of the use of the service, including, without limitation, any of such damages arising out of or in connection with mistakes, omissions, interruptions, delays, errors, defects, loss of data, loss of profits, loss of business or anticipatory profits, whether such damages are asserted in an action brought in contract, in tort or pursuant to some other theory and whether the possibility of such damages was made known or was foreseeable.

The terms of this section shall survive the termination of this agreement for whatever reason.

In no event shall HRTec’s entire liability exceed the total amount paid by the Participating Entity to HRTec under this agreement.

7. **Rights and License in and to the Participating Entity and End User Data**

All rights, including Intellectual Property Rights, in and to the Participating Entity and End User Data will remain the exclusive property of the Participating Entity, and HRTec will retain a limited, nonexclusive license to access and use these Data as provided in the NASPO Master

Agreement, the Exhibits thereof, and the executed Participating Addendum solely to perform its obligations to the NASPO Master Agreement and the Participating Addendum.

This Agreement does not give either party any rights, implied or otherwise, to the other's Data, content, or intellectual property, except as expressly stated in the Service Agreement and Participating Addendum.

The Participating Entity retains the right to use FedHIVE Cloud Computing services to access and retrieve Participating Entity and End User Data stored on the FedHIVE infrastructure at any time at its sole discretion.

8. Data Privacy

HRTec will use Participating Entity Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for the Participating Entity and its End Users sole benefit and will not share such Data with or disclose it to any Third Party without the prior written consent of the Participating Entity or as otherwise required by law. By way of illustration and not of limitation, HRTec will not use such Data for HRTec's own benefit and will not engage in "data mining" of Participating Entity or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the Participating Entity.

All Participating Entity and End User Data will be stored on servers located solely within the Continental United States.

HRTec will provide access to Participating Entity and End User Data only to those HRTec employees, contractors and subcontractors ("HRTec Staff") who need to access the Data to fulfill HRTec's obligations under this Agreement. HRTec will ensure that, prior to being granted access to the Data, HRTec Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

The Participating Entity represents that it is subject to all applicable federal and state laws restricting the access, use and disclosure of Protected Information and all the terms and conditions contained in the NASPO Master Agreement and the Participating Addendum.

9. Data Security and Integrity

All HRTec facilities used to store and process Participating Entity and End User Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such Data from unauthorized access, destruction, use, modification, or disclosure. Such measures will be no less protective than those used to secure HRTec's own Data of a similar type, and in no event less than reasonable in view of the type and nature of the Data involved.

HRTec shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of FedHIVE Cloud Computing Services to the Participating Entity in a manner that is, at all times during the term of this Agreement, at a level equal to or

more stringent than those specified in the NASPO Master Agreement, and Participating Addendum which is incorporated herein by reference.

Without limiting the foregoing, HRTec warrants that all Participating Entity Data and End User Data will be encrypted in transmission (including via web interface) and in storage at a level equivalent to or stronger than 256-bit level encryption.

HRTec shall at all times use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting methods in providing Services under this Agreement.

HRTec will configure the Services to filter spam while permitting communications from Third Party Internet Protocol addresses identified by the Participating Entity as legitimate.

Prior to the Effective Date of this Agreement, HRTec will at its expense conduct or have conducted the following, and thereafter, HRTec will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise:

(a) A Third-Party Assessment Organization (3PAO) audit of Supplier's security policies, procedures and controls

(b) Certification under FedRAMP and/or Cloud Security Alliance Security Trust and Assurance Registry (CSA STAR) attestation and certification

(c) A vulnerability scan, performed by a HRTec and FedRAMP approved Third Party scanner, of HRTec's systems and facilities that are used in any way to deliver FedHIVE Cloud Computing Services under this Agreement

(d) A formal penetration test, performed by the process and qualified personnel approved by HRTec and the Participating Entity, of HRTec's systems and facilities that are used in any way to deliver FedHIVE Cloud Computing Services under this Agreement.

HRTec will provide the Participating Entity the reports or other documentation resulting from the above audits, certifications, scans and tests.

Based on the results of the above audits, certifications, scans and tests, HRTec will promptly modify its security measures in order to meet its obligations under this Agreement and provide the Participating Entity with written evidence of remediation.

The Participating Entity may require, at its expense, that HRTec perform additional audits and tests, the results of which will be provided to the Participating Entity within seven (7) business days of receipt of such results.

HRTec shall protect the Participating Entity and End User Data against deterioration or degradation of Data quality and authenticity, including, but not limited to annual Third-Party Data integrity audits. HRTec will provide the Participating Entity the results of the above audits, along with a plan for addressing or resolving any shortcomings identified by such audits.

10. Response to Legal Orders, Demands or Requests for Data

Except as otherwise expressly prohibited by law, HRTec will:

(a) If required by a court of competent jurisdiction or an administrative body to disclose Participating Entity and/or End User Data, HRTec will notify the Participating Entity in writing immediately upon receiving notice of such requirement and prior to any such disclosure

(b) Consult with the Participating Entity regarding its response

(c) Cooperate with Participating Entity reasonable requests in connection with efforts by the Participating Entity to intervene and quash or modify the legal order, demand or request

(d) Upon Participating Entity request, provide the Participating Entity with a copy of its response.

If the Participating Entity receives a subpoena, warrant, or other legal order, demand or request seeking Participating Entity or End User Data maintained by HRTec, the Participating Entity will promptly provide a copy to HRTec. HRTec will supply the Participating Entity with copies of Data required for the Participating Entity to respond within forty-eight (48) hours after receipt of copy from the Participating Entity, and will cooperate with reasonable requests from the Participating Entity in connection with its response.

11. Service Levels

HRTec represents and warrants that FedHIVE Cloud Computing Services will be performed in a professional manner consistent with industry standards reasonably applicable to such Services.

HRTec represents and warrants that FedHIVE Cloud Computing Services will be operational at least 99.9% of the time in any given month during the term of this Agreement, meaning that the outage or Downtime percentage will be not more than 0.1%. Excluding mutually agreed upon maintenance windows to be defined in the Participating Addendum.

If the Services availability falls below 99.9% in any month, HRTec shall provide the Participating Entity with a credit of that month's bill for services according to the table below.

AVAILABILITY PERCENTAGE	PERCENTAGE OF CREDIT
99.6% to 99.8%	5%
99.4% to 99.59%	10%
99.0% to 99.39%	15%
97.0% to 98.9%	20%
Below 97.0%	25%

HRTec represents and warrants that ninety-five percent (95%) of all transactions shall process within no more than one (1) second, and no single transactions shall take longer than five (5) seconds to process.

If HRTec's system response times fall below the warranted level for two (2) or more consecutive weeks, HRTec shall provide the Participating Entity with a credit in the amount of twenty percent (20%) of the Services fees for that month.

HRTec shall provide the Participating Entity with any credits resulting from all unachieved service levels in the form of credit provided to the Participating Entity on the invoice for the month following the month in which the service levels were not achieved.

HRTec shall provide the Participating Entity with monthly reports documenting its compliance with the service levels detailed herein. Reports shall include, but not be limited to, providing the following information:

(a) Monthly Services availability by percent time, dates and minutes that Services were not available, and identification of months in which agreed upon service levels were not achieved

(b) Average transaction processing time per week, the fastest and slowest individual transaction processing time per week, the percent of transactions processed that meet the service levels stated herein, and identification of weeks in which agreed upon service levels are not met.

The Participating Entity may, at its own expense, retain a Third Party to validate HRTec's performance in meeting agreed upon service levels.

12. Entire Agreement

This Agreement, together with all the incorporated NASPO and Participating Entity Agreements, exhibits, schedules, attachments, and proposals and addenda, constitutes the entire, final and exclusive Agreement between the parties with respect to the subject matter herein and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions, whether oral or written, between the parties. The parties expressly disclaim the right to claim the enforceability or effectiveness of any oral modifications to this Agreement or any amendments based on course of dealing, waiver, release, estoppel or other similar legal theory. No click-through, or other end user terms and conditions or agreements ("Additional Terms") provided with any FedHIVE Cloud Computing Services or products hereunder shall be binding on the Participating Entity or its End Users, even if use of such FedHIVE Cloud Computing Services or products requires an affirmative "acceptance" of those Additional Terms before access is permitted. All such Additional Terms shall be of no force and effect and shall be deemed rejected by the Participating Entity in their entirety. Any amendment or modification to this Agreement shall be effective only if in writing and signed by duly authorized representatives of both HRTec and the Participating Entity. The authorized signatory from each party has read the Agreement, understands it and is authorized to bind his/her organization. This Agreement becomes binding when signed by the authorized signatory of both parties.

FedHIVE CUSTOMER SUPPORT POLICY

This Customer Support Policy governs the support that HRTec provides for FedHIVE Cloud Computing Services. This Policy may be updated from time to time.

1. **Scope**

The purpose of Customer Support is to resolve defects that cause the FedHIVE Cloud Computing Service to not perform in conformance to the Service Agreement as incorporated by the Participating Addendum. A resolution to a defect may consist of a fix, workaround or other relief HRTec deems reasonable.

Customer Support does not include:

- implementation services
- configuration services
- integration services
- customization services or other custom software development
- training
- assistance with administrative functions

Customer Support is not required to provide resolutions for immaterial defects or defects due to modifications of the FedHIVE Cloud made by any person other than HRTec or a person acting at HRTec direction.

2. Support Provisions

The following provisions shall be applicable to the correction of FedHIVE Cloud Computing Services errors:

(a) If the Participating Entity detects what it considers to be an error in the FedHIVE Cloud Computing Services which causes it not to conform to, or produce results in accordance with, the Participating Addendum, then the Participating Entity shall by telephone or e-mail notify HRTec of the error.

(b) HRTec shall respond within two (2) hours to the Participating Entity initial request for assistance in correcting or creating a workaround for a FedHIVE Cloud Computing Services error. HRTec's response shall include assigning fully-qualified technicians to work with the Participating Entity to diagnose and correct or create a workaround for the FedHIVE Cloud Computing Services error and notifying the Participating Entity representative making the initial request for assistance of HRTec's efforts, plans for resolution of the error, and estimated time required to resolve the error.

(c) For Class 1 Errors, within twenty-four (24) hours after the Participating Entity first reports the error, HRTec will provide a correction or workaround acceptable to the Participating Entity. HRTec's correction process will include assigning fully-qualified technicians to work with the Participating Entity without interruption or additional charge.

(d) If HRTec fails to provide a reasonable correction or workaround for a Class 1 Error within twenty-four (24) hours, HRTec shall provide a price adjustment reflecting the reduction of value the Participating Entity will incur as a result of the Class 1 Error and not as a penalty or compensation for damage, the sum of 1/365 of the technical support fees, expressed as an annual charge, for each additional day or part thereof that HRTec fails to provide a reasonable correction or workaround for the Class 1 Error. HRTec will provide such payment in the form of a credit provided to the Participating Entity no later than the following month's invoice.

(e) The Project Managers, or such persons as otherwise designated by the Participating Entity and HRTec, shall serve as said parties' contacts for all communications relating to technical support. Each party may change its own contact person by written notice to the other party.

3. Business Hours

Customer Support is available by phone or email from 7am eastern to 6pm pacific 7 days a week.

4. Access Contacts

Customer may contact FedHIVE support using one of the following means:

• Email to help@fedhive.com.

• Phone to 571-257-0138.

5. Customer Responsibilities

Customer's obligations are as follows:

(a) Customer agrees to receive from HRTec communications via email or phone.

(b) Customer shall appoint no more than five (5) contacts ("Customer Authorized Contacts") to engage Customer Support for questions and/or technical issues.

(c) Customer shall cooperate to enable HRTec to deliver the FedHIVE Cloud Computing Service and support for the service.

(d) Customer is solely responsible for the use of the FedHIVE Cloud Computing Service by its authorized users.

Discern Software Service Agreement for NASPO ValuePoint Customers

1. **Scope**
   This agreement applies to any service or combination of services ordered by the Participating Entity and provided by HRTec to customer that involves the provision of Discern SaaS Suite services applications and data used by the Participating Entity (collectively, "the service"). The types of services include but are not limited to the Discern SaaS Suite Offerings proposed for the NASPO MSA, EEO Manager and SCA&R Manager, provisioned for customers/agencies within HRTec's FedHIVE cloud infrastructure. These SaaS applications are accessible by authorized users from customer approved devices via web-browser interface.
2. **Modifications to this Agreement**
   This Service Agreement is designed to be supplemental to the NASPO ValuePoint Master Service Agreement and Exhibits 2 and 3 thereof. This Service Agreement may be revised to incorporate changes, additions, and /or deletions resulting from Participating Entity negotiations for inclusion/exclusion in an executed Participating Addendum.
3. **Termination**
   Participating Entities may terminate this Service Agreement per the terms of the NASPO Master Agreement paragraph 7 and the executed Participating Addendum. HRTec shall provide for data preservation and/or disposition per paragraph 7 of the Exhibits 2 and 3, unless specified otherwise in the executed Participating Agreement.
4. **Term, Billing Cycle, and Renewal Term**
   The term, billing cycle, and renewal term of this Service Agreement shall be specified in the executed Participating Addendum.
5. **Access and Use**
   Subject to the terms and conditions contained in this Agreement, HRTec agrees to provide the features and functions of Discern SaaS Suite Services in connection with one or more Participating Entity Applications (as identified in an applicable Participating Addendum Exhibit) during the Participating Addendum Term, solely for use by the Participating Entity, its Authorized Entity(ies) and its End Users, solely in accordance with any documentation provided by HRTec. The Participating Entity acknowledges and agrees that, as between the Participating Entity and HRTec, the Participating Entity shall be responsible for all acts and omissions of Authorized Entities, and any act or omission by an Authorized Entity which, if undertaken by the Participating Entity, would constitute a breach of this Addendum, shall be deemed a breach of this Addendum by the Participating Entity.
6. **Disclaimer of Warranties/Limitation of Liability**
   Except as explicitly provided for in the NASPO Master Agreement, Exhibits 2 and 3 thereof, and the Participating Addendum, HRTec hereby expressly disclaims all warranties of any nature, express, implied or otherwise, including but not limited to any implied warranties of merchantability, noninfringement, or fitness for a particular purpose. HRTec does not

guarantee or warranty the deliverability of any data generated by, hosted by or otherwise passed through HRTec owned or operated equipment or computer systems. The Participating Entity expressly agrees that HRTec shall not be liable for damages of any kind which arise directly or indirectly out of the non-delivery of data generated by, hosted by or otherwise passed through HRTec owned or operated equipment or computer systems.

HRTec is a distributor and not a publisher of the content supplied by customer; as such, HRTec exercises no editorial control over such content. The Participating Entity agrees to indemnify, defend and hold HRTec and its affiliates, partners and licensors and each of their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses arising out of or in connection with any claim arising out of (a) Participating Entity use of the service in a manner not authorized by this agreement, and/or in violation of the applicable restrictions, acceptable use policy, and/or applicable law and (b) Participating Entity or Participating Entity employees or representatives negligence or willful misconduct.

Participating Entity expressly agrees that HRTec shall not be liable for damages of any kind, including but not limited to special, incidental, and/or consequential damages (including, without limitation, costs of procuring substitute products or services) which arise directly or indirectly out of the use of the service, including, without limitation, any of such damages arising out of or in connection with mistakes, omissions, interruptions, delays, errors, defects, loss of data, loss of profits, loss of business or anticipatory profits, whether such damages are asserted in an action brought in contract, in tort or pursuant to some other theory and whether the possibility of such damages was made known or was foreseeable.

The terms of this section shall survive the termination of this agreement for whatever reason.

In no event shall HRTec’s entire liability exceed the total amount paid by the Participating Entity to HRTec under this agreement.

7. Rights and License in and to the Participating Entity and End User Data

All rights, including Intellectual Property Rights, in and to the Participating Entity and End User Data will remain the exclusive property of the Participating Entity, and HRTec will retain a limited, nonexclusive license to access and use these Data as provided in the NASPO Master Agreement, the Exhibits thereof, and the executed Participating Addendum solely to perform its obligations to the NASPO Master Agreement and the Participating Addendum.

This Agreement does not give either party any rights, implied or otherwise, to the other’s Data, content, or intellectual property, except as expressly stated in the Service Agreement and Participating Addendum.

The Participating Entity retains the right to use Discern SaaS Suite services to access and retrieve Participating Entity and End User Data stored on the Discern SaaS Suite products at any time at its sole discretion.

8. Data Privacy

HRTec will use Participating Entity Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for the Participating Entity and its End Users sole benefit and will not share such Data with or disclose it to any Third Party without the prior written consent of the Participating Entity or as otherwise required by law. By way of illustration and not of limitation, HRTec will not use such Data for HRTec's own benefit and will not engage in "data mining" of Participating Entity or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the Participating Entity.

All Participating Entity and End User Data will be stored on servers located solely within the Continental United States.

HRTec will provide access to Participating Entity and End User Data only to those HRTec employees, contractors and subcontractors ("HRTec Staff") who need to access the Data to fulfill HRTec's obligations under this Agreement. HRTec will ensure that, prior to being granted access to the Data, HRTec Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

The Participating Entity represents that it is subject to all applicable federal and state laws restricting the access, use and disclosure of Protected Information and all the terms and conditions contained in the NASPO Master Agreement and the Participating Addendum.

9. Data Security and Integrity

All HRTec facilities used to store and process Participating Entity and End User Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such Data from unauthorized access, destruction, use, modification, or disclosure. Such measures will be no less protective than those used to secure HRTec's own Data of a similar type, and in no event less than reasonable in view of the type and nature of the Data involved.

HRTec shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of Discern SaaS Suite Services to the Participating Entity in a manner that is, at all times during the term of this Agreement, at a level equal to or more stringent than those specified in the NASPO Master Agreement, and Participating Addendum which is incorporated herein by reference.

Without limiting the foregoing, HRTec warrants that all Participating Entity Data and End User Data will be encrypted in transmission (including via web interface) and in storage at a level equivalent to or stronger than 256-bit level encryption.

HRTec shall at all times use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting methods in providing Services under this Agreement.

HRTec will configure the Services to filter spam while permitting communications from Third Party Internet Protocol addresses identified by the Participating Entity as legitimate.

Prior to the Effective Date of this Agreement, HRTec will at its expense conduct or have conducted the following, and thereafter, HRTec will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise:

(a) A Third-Party Assessment Organization (3PAO) audit of Supplier's security policies, procedures and controls

(b) Certification under FedRAMP and/or Cloud Security Alliance Security Trust and Assurance Registry (CSA STAR) attestation and certification

(c) A vulnerability scan, performed by a HRTec and FedRAMP approved Third Party scanner, of HRTec's systems and facilities that are used in any way to deliver Discern SaaS Suite Services under this Agreement

(d) A formal penetration test, performed by the process and qualified personnel approved by HRTec and the Participating Entity, of HRTec's systems and facilities that are used in any way to deliver Discern SaaS Suite Services under this Agreement.

HRTec will provide the Participating Entity the reports or other documentation resulting from the above audits, certifications, scans and tests.

Based on the results of the above audits, certifications, scans and tests, HRTec will promptly modify its security measures in order to meet its obligations under this Agreement and provide the Participating Entity with written evidence of remediation.

The Participating Entity may require, at its expense, that HRTec perform additional audits and tests, the results of which will be provided to the Participating Entity within seven (7) business days of receipt of such results.

HRTec shall protect the Participating Entity and End User Data against deterioration or degradation of Data quality and authenticity, including, but not limited to annual Third-Party Data integrity audits. HRTec will provide the Participating Entity the results of the above audits, along with a plan for addressing or resolving any shortcomings identified by such audits.

10. Response to Legal Orders, Demands or Requests for Data

Except as otherwise expressly prohibited by law, HRTec will:

(a) If required by a court of competent jurisdiction or an administrative body to disclose Participating Entity and/or End User Data, HRTec will notify the Participating Entity in writing immediately upon receiving notice of such requirement and prior to any such disclosure

(b) Consult with the Participating Entity regarding its response

(c) Cooperate with Participating Entity reasonable requests in connection with efforts by the Participating Entity to intervene and quash or modify the legal order, demand or request

(d) Upon Participating Entity request, provide the Participating Entity with a copy of its response.

If the Participating Entity receives a subpoena, warrant, or other legal order, demand or request seeking Participating Entity or End User Data maintained by HRTec, the Participating Entity will promptly provide a copy to HRTec. HRTec will supply the Participating Entity with copies of Data required for the Participating Entity to respond within forty-eight (48) hours after receipt of copy from the Participating Entity, and will cooperate with reasonable requests from the Participating Entity in connection with its response.

11. Service Levels

HRTec represents and warrants that Discern SaaS Suite Services will be performed in a professional manner consistent with industry standards reasonably applicable to such Services. HRTec represents and warrants that Discern SaaS Suite Services will be operational at least 99.9% of the time in any given month during the term of this Agreement, meaning that the outage or Downtime percentage will be not more than 0.1%. Excluding mutually agreed upon maintenance windows to be defined in the Participating Addendum.

If the Services availability falls below 99.9% in any month, HRTec shall provide the Participating Entity with a credit of that month's bill for services according to the table below.

AVAILABILITY PERCENTAGE	PERCENTAGE OF CREDIT
99.6% to 99.8%	5%
99.4% to 99.59%	10%
99.0% to 99.39%	15%
97.0% to 98.9%	20%
Below 97.0%	25%

HRTec represents and warrants that ninety-five percent (95%) of all transactions shall process within no more than one (1) second, and no single transactions shall take longer than five (5) seconds to process.

If HRTec's system response times fall below the warranted level for two (2) or more consecutive weeks, HRTec shall provide the Participating Entity with a credit in the amount of twenty percent (20%) of the Services fees for that month.

HRTec shall provide the Participating Entity with any credits resulting from all unachieved service levels in the form of credit provided to the Participating Entity on the invoice for the month following the month in which the service levels were not achieved.

HRTec shall provide the Participating Entity with monthly reports documenting its compliance with the service levels detailed herein. Reports shall include, but not be limited to, providing the following information:

(a) Monthly Services availability by percent time, dates and minutes that Services were not available, and identification of months in which agreed upon service levels were not achieved

(b) Average transaction processing time per week, the fastest and slowest individual transaction processing time per week, the percent of transactions processed that meet the service levels stated herein, and identification of weeks in which agreed upon service levels are not met.

The Participating Entity may, at its own expense, retain a Third Party to validate HRTec's performance in meeting agreed upon service levels.

12. Entire Agreement

This Agreement, together with all the incorporated NASPO and Participating Entity Agreements, exhibits, schedules, attachments, and proposals and addenda, constitutes the entire, final and exclusive Agreement between the parties with respect to the subject matter herein and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions, whether oral or written, between the parties. The parties expressly disclaim the right to claim the enforceability or effectiveness of any oral modifications to this Agreement or any amendments based on course of dealing, waiver, release, estoppel or other similar legal theory. No click-through, or other end user terms and conditions or agreements ("Additional Terms") provided with any Discern SaaS Suite Services or products hereunder shall be binding on the Participating Entity or its End Users, even if use of such Discern SaaS Suite Services or products requires an affirmative "acceptance" of those Additional Terms before access is permitted. All such Additional Terms shall be of no force and effect and shall be deemed rejected by the Participating Entity in their entirety. Any amendment or modification to this Agreement shall be effective only if in writing and signed by duly authorized representatives of both HRTec and the Participating Entity. The authorized signatory from each party has read the Agreement, understands it and is authorized to bind his/her organization. This Agreement becomes binding when signed by the authorized signatory of both parties.

DISCERN SAAS SUITE CUSTOMER SUPPORT POLICY

This Customer Support Policy governs the support that HRTec provides for Discern SaaS Suite Services. This Policy may be updated from time to time.

1. **Scope**

The purpose of Customer Support is to resolve defects that cause the Discern SaaS Suite Service products to not perform in conformance to the Service Agreement as incorporated by the Participating Addendum. A resolution to a defect may consist of a fix, workaround or other relief HRTec deems reasonable.

Customer Support does not include:

- implementation services
- configuration services
- integration services
- customization services or other custom software development
- training
- assistance with administrative functions

Customer Support is not required to provide resolutions for immaterial defects or defects due to modifications of Discern SaaS Suite products made by any person other than HRTec or a person acting at HRTec direction.

2. Support Provisions

The following provisions shall be applicable to the correction of Discern SaaS Suite Services errors:

(a) If the Participating Entity detects what it considers to be an error in the Discern SaaS Suite Services which causes it not to conform to, or produce results in accordance with, the Participating Addendum, then the Participating Entity shall by telephone or e-mail notify HRTec of the error.

(b) HRTec shall respond within two (2) hours to the Participating Entity initial request for assistance in correcting or creating a workaround for a Discern SaaS Suite Services error. HRTec's response shall include assigning fully-qualified technicians to work with the Participating Entity to diagnose and correct or create a workaround for the Discern SaaS Suite Services error and notifying the Participating Entity representative making the initial request for assistance of HRTec's efforts, plans for resolution of the error, and estimated time required to resolve the error.

(c) For Class 1 Errors, within twenty-four (24) hours after the Participating Entity first reports the error, HRTec will provide a correction or workaround acceptable to the Participating Entity. HRTec's correction process will include assigning fully-qualified technicians to work with the Participating Entity without interruption or additional charge.

(d) If HRTec fails to provide a reasonable correction or workaround for a Class 1 Error within twenty-four (24) hours, HRTec shall provide a price adjustment reflecting the

reduction of value the Participating Entity will incur as a result of the Class 1 Error and not as a penalty or compensation for damage, the sum of 1/365 of the technical support fees, expressed as an annual charge, for each additional day or part thereof that HRTec fails to provide a reasonable correction or workaround for the Class 1 Error. HRTec will provide such payment in the form of a credit provided to the Participating Entity no later than the following month's invoice.

(e) The Project Managers, or such persons as otherwise designated by the Participating Entity and HRTec, shall serve as said parties' contacts for all communications relating to technical support. Each party may change its own contact person by written notice to the other party.

3. Business Hours

Customer Support is available by phone or email from 7am eastern to 6pm pacific 7 days a week.

4. Access Contacts

Customer may contact support using one of the following means:

• Email to help@fedhive.com.

• Phone to 571-257-0138.

5. Customer Responsibilities

Customer's obligations are as follows:

(a) Customer agrees to receive from HRTec communications via email or phone.

(b) Customer shall appoint no more than five (5) contacts ("Customer Authorized Contacts") to engage Customer Support for questions and/or technical issues.

(c) Customer shall cooperate to enable HRTec to deliver the Discern SaaS Suite Service and support for the service.

(d) Customer is solely responsible for the use of the Discern SaaS Suite Service by its authorized users.