

STATE OF VERMONT PARTICIPATING ADDENDUM #37902  
FOR NASPO VALUEPOINT PURCHASING PROGRAM: CLOUD SOLUTIONS

Led by the State of Utah

**Master Agreement #AR2476**

**Contractor:** CherryRoad Technologies Inc.

**Contractor's NASPO ValuePoint Webpage:** <https://www.naspovaluepoint.org/portfolios/portfolio-contractor/cherryroad/>

1. **Parties.** This Participating Addendum is a contract between the State of Vermont, through its Department of Buildings and General Services, Office of Purchasing & Contracting (hereinafter "State" or "Vermont"), and the Contractor identified above. It is the Contractor's responsibility to contact the Vermont Department of Taxes to determine if, by law, the Contractor is required to have a Vermont Department of Taxes Business Account Number.
2. **Subject Matter.** This Participating Addendum authorizes the purchase of Cloud Solutions from Contractor pursuant to the Master Agreement identified above, which is hereby incorporated by reference. Contractor's awarded categories are:
  - a. **Platform as a Service (PaaS):** As used in the Participation Addendum 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.
  - b. **Infrastructure as a Service (IaaS):** As used in the Participation Addendum 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).
  - c. **Software as a Service (SaaS):** As used in this Participation Addendum 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.
3. **Definitions.** Capitalized terms used, but not defined herein, have the meanings ascribed to such terms in the Master Agreement between the Lead State and the Contractor.
4. **Purchasing Entities.** This Participating Addendum may be used by (a) all departments, offices, institutions, and other agencies of the State of Vermont and counties (each a "State Purchaser") according to the process for ordering and other restrictions applicable to State Purchasers set forth

herein; and (b) political subdivisions of the State of Vermont and any institution of higher education chartered in Vermont and accredited or holding a certificate of approval from the State Board of Education as authorized under 29 V.S.A. § 902 (each an “Additional Purchaser”). Issues concerning interpretation and eligibility for participation are solely within the authority of the State of Vermont Chief Procurement Officer. The State of Vermont and its officers and employees shall have no responsibility or liability for Additional Purchasers. Each Additional Purchaser is to make its own determination whether this Participating Addendum and the Master Agreement are consistent with its procurement policies and regulations.

5. ***Contract Term.*** The period of Contractor’s performance shall begin on April 1, 2019 and end upon expiration of the Master Agreement, unless terminated earlier in accordance with the terms of this Participating Addendum or the Master Agreement. An amendment to this Participating Addendum shall not be necessary in the event of the renewal or extension of the Master Agreement.
6. ***Available Products and Services.*** All products, services and accessories listed on the Contractor’s NASPO ValuePoint Webpage may be purchased under this Participating Addendum.
7. ***No Lease Agreements.*** Contractor is prohibited from leasing to State Purchasers under this Participating Addendum. Additional Purchasers are not subject to this prohibition and may negotiate lease agreements with Contractor if the terms of the Master Agreement permit leasing.
8. ***Requirements for Ordering.***
  - a. Orders made under this Participating Addendum must include a specifically-negotiated Statement of Work or Service Level Agreement terms as necessary for the Product and/or Service to meet the Purchasing Entity’s requirements. Orders funded by federal funds may include additional terms as necessary to comply with federal requirements.
    - i. Prior to entering into Statement of Work or Service Level Agreement with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and/or Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.
  - b. State Purchasers must follow the ordering procedures of the State Contract Administrator to execute orders against this Participating Addendum, which shall include, as applicable, obtaining approval from the State CIO and/or Attorney General’s Office prior to making purchases under this Participating Addendum.
  - c. The State’s Agency of Digital Services Procurement Office is the only entity authorized to place orders on behalf of State Purchasers. Contractor agrees that it will not accept or fulfill orders placed on behalf of State Purchasers from any other source. Contractor’s failure to meet this requirement may result in suspension or termination of this Participating Addendum.
  - d. All orders placed under this Participating Addendum must include the Participating Addendum Number on the Purchase Order.

9. ***Payment Provisions and Invoicing.***

**Contractor:** CherryRoad Technologies Inc.

- a. Product offerings and complete details of product pricing, including discounts, applicable to this Participating Addendum are set forth in the Price Schedule maintained on-line at Contractor's NASPO ValuePoint Webpage listed above.
- b. Purchasing Entities may solicit the Contractor or Fulfillment Partner/Authorized Reseller for deeper discounts than the minimum contract pricing as set forth in the Price Schedule (e.g., additional volume pricing, incremental discounts, firm fixed pricing or other incentives).
- c. If applicable, all equipment pricing is to include F.O.B. delivery to the ordering facility. No request for extra delivery cost will be honored.
- d. In the discretion of the Purchasing Entity, retainage may be specified in a Purchase Order, in an amount mutually agreeable to the parties.
- e. Payment terms are Net 30 days from the date the State receives an error-free invoice with all necessary and complete supporting documentation. Invoices shall itemize all work performed during the invoice period, including, as applicable, the dates of service, rates of pay, hours of work performed, and any other information and/or documentation appropriate and sufficient to substantiate the amount invoiced for payment. As applicable, a copy of the notice(s) of acceptance shall accompany invoices submitted for payment.
- f. Invoices shall be sent to the address identified on the Purchasing Entity's Purchase Order and shall specify the address to which payments will be sent. The State of Vermont Participating Addendum Number and Purchasing Entity's Purchase Order Number shall appear on each invoice for all purchases placed under this Participating Addendum.
- g. Reimbursement of expenses is not authorized. All rates set forth in a Purchase Order shall be inclusive of any and all Contractor fees and expenses.
- h. Unopened Products can be returned with no restocking fee up to 30 days from the date of receipt.
- i. The State Purchasing Card may be used by State Purchasers for the payment of invoices. Use of the Purchasing Card requires all required documentation applicable to the purchase. The Purchasing Card is a payment mechanism, not a procurement approach and, therefore, does not relieve State Purchasers from adhering to all procurement laws, regulations, policies, procedures, and best practices.

**10. *Fulfillment Partners/Authorized Resellers.***

- a. Resellers (or Fulfillment Partners) are available for this Participating Addendum if and to the extent approved by the State Chief Procurement Officer (each an "Authorized Reseller"). Any Authorized Resellers will be listed on the Contractor's NASPO ValuePoint Webpage listed above.
  - i. The State does not intend to approve resellers or fulfillment partners for this Participating Addendum except as required to provide services for certain Products (e.g., where a Product requires a managed service provider or other such services that Contractor is unable to provide without engaging a third party). Contractor shall notify the State when a Product requested by a Vermont Purchasing Entity will require

**Contractor:** CherryRoad Technologies Inc.

engagement of a third party. The State Chief Procurement Officer may, in its discretion, approve the third-party engagement on a limited basis, for the specific purchase only, or on a general basis, for whenever such Product is purchased under this Participating Addendum.

- ii. A reseller or fulfillment partner approved by the State for this Participating Addendum is expressly not authorized to invoice State Purchasers directly. This provision shall not apply to Additional Purchasers.
  - b. All State policies, guidelines and requirements shall apply to Authorized Resellers.
  - c. Contractor shall be responsible for successful performance and compliance with all requirements in accordance with the terms and conditions set forth by this Participating Addendum. Contractor acknowledges that each and all of the promises it makes as “Contractor” in the Master Agreement and in this Participating Addendum will apply to all Products and Services provided hereunder, regardless of who is providing or licensing the Product or performing the work.
    - i. Contractor promises that Purchasing Entities will not be required to affirmatively accept additional terms and conditions to use or access any Product or Service purchased under this Participating Addendum, whether by electronic means (e.g., click-through) or otherwise.
    - ii. Contractor promises that each of the third parties whose Products and/or Services are available for purchase under this Participating Addendum understand and agree that the terms and conditions applicable to their Products and/or Services are as set forth in the Master Agreement, as amended, and are subordinate to the terms of this Participating Addendum and the NASPO ValuePoint Master Agreement Terms & Conditions and associated service model Exhibits.
11. **Reporting.** Contractor shall submit quarterly reports electronically in the same format as set forth under the Master Agreement, detailing the purchasing of all items under this Participating Addendum. Contractor’s reporting shall state "no activity" for any month in which there is no activity during a quarterly reporting period.
- a. The reports shall be an excel spreadsheet transmitted electronically to [SOV.ThePathForward@state.vt.us](mailto:SOV.ThePathForward@state.vt.us).
  - b. Reports are due for each quarter as follows:

Reporting Period	Report Due
January 1 to March 31	April 30
April 1 to June 30	July 31
July 1 to September 30	October 31
October 1 to December 31	January 31



**Contractor:** CherryRoad Technologies Inc.

- c. Failure to meet these reporting requirements may result in suspension or termination of this Participating Addendum.
12. **Prior Approvals.** In accordance with current State law, bulletins, and interpretations, this Participating Addendum shall not be binding until it has been approved by the Vermont Attorney General's Office, the Secretary of Administration, and the State's Chief Information Officer.
13. **Amendment.** No changes, modifications, or amendments in the terms and conditions of this Participating Addendum shall be effective unless reduced to writing, numbered and signed by the duly authorized representative of the State and Contractor.
14. **Termination.** This Participating Addendum may be terminated by the State at any time upon 30 days prior written notice to the Contractor. Upon termination or expiration of this Participating Addendum, each party will assist the other in orderly termination of the Participating Addendum and the transfer of all assets, tangible and intangible, as may facilitate the orderly, non-disrupted business continuation of each party. This provision shall not relieve the Contractor of the obligation to perform under any order executed prior to the effective date of termination or other expiration of this Participating Addendum.
15. **Primary Contacts.** The Parties will keep and maintain current at all times a primary point of contact for this Participating Addendum. The primary contacts for this this Participating Addendum are as follows:

a. **For the Contractor:**

Name: Christopher Tilden  
Phone: 609/353-8001  
Email: [CTilden@cherryroad.com](mailto:CTilden@cherryroad.com)

b. **For the State:**

Name: State of Vermont, Stephen Fazekas  
Address: 109 State Street, Montpelier, VT 05633-3001  
Phone: 802/828-2210  
Fax: 802/828-2222  
Email: [Stephen.fazekas@vermont.gov](mailto:Stephen.fazekas@vermont.gov)

**16. Additional Terms and Conditions.**

- a. Notwithstanding any contrary language anywhere, in no event shall the terms of this contract or any document furnished by Contractor in connection with performance under this contract obligate the State to (1) defend or indemnify Contractor or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of Contractor or any third party.
- b. If required by an order made by a State Purchaser under this Participating Addendum, the terms and conditions of the State of Vermont Business Associate Agreement, revised July 7, 2017 (the six-page document available online at: <https://bgs.vermont.gov/sites/bgs/files/files/purchasing->

**Contractor:** CherryRoad Technologies Inc.

[contracting/contracts/Attachment E BAA HIPAA 071717REV.doc](#)) shall be incorporated by reference and apply to the order. This provision shall not apply to Additional Purchasers.

- c. Contractor is required at all times to comply with all applicable federal and state laws and regulations pertaining to information security and privacy.
- d. **Governing Law, Jurisdiction and Venue; No Waiver of Jury Trial:** This Agreement will be governed by the laws of the State of Vermont. Any action or proceeding brought by either the State or the Contractor in connection with this Agreement shall be brought and enforced in the Superior Court of the State of Vermont, Civil Division, Washington Unit. Contractor irrevocably submits to the jurisdiction of this court for any action or proceeding regarding this Agreement. Contractor agrees that it must first exhaust any applicable administrative remedies with respect to any cause of action that it may have against the State with regard to its performance under this Agreement. Contractor agrees that the State shall not be required to submit to binding arbitration or waive its right to a jury trial.
- e. **Sovereign Immunity:** The State reserves all immunities, defenses, rights or actions arising out of the State's sovereign status or under the Eleventh Amendment to the United States Constitution. No waiver of the State's immunities, defenses, rights or actions shall be implied or otherwise deemed to exist by reason of the State's entry into this Agreement.
- f. **False Claims Act:** Contractor acknowledges that it is subject to the Vermont False Claims Act as set forth in 32 V.S.A. § 630 *et seq.* Contractor's liability to the State under the False Claims Act shall not be limited notwithstanding any agreement of the State to otherwise limit Contractor's liability.
- g. **Whistleblower Protections:** Contractor shall not discriminate or retaliate against one of its employees or agents for disclosing information concerning a violation of law, fraud, waste, abuse of authority or acts threatening health or safety, including but not limited to allegations concerning the False Claims Act. Further, Contractor shall not require such employees or agents to forego monetary awards as a result of such disclosures, nor should they be required to report misconduct to Contractor or its agents prior to reporting to any governmental entity and/or the public.
- h. **Fair Employment Practices and Americans with Disabilities Act:** Contractor agrees to comply with the requirement of 21 V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable. Contractor shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by Contractor under this Agreement.
- i. **Set Off:** The State may set off any sums which Contractor owes the State against any sums due Contractor under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures set forth in 32 V.S.A. § 3113.
- j. **Taxes Due to the State:** Contractor certifies under the pains and penalties of perjury that, as of the date this Agreement is signed, Contractor is in good standing with respect to, or in full compliance with, a plan to pay any and all taxes due the State of Vermont.

**Contractor:** CherryRoad Technologies Inc.

- k. **Taxation of Purchases:** All State purchases must be invoiced tax free. An exemption certificate will be furnished upon request with respect to otherwise taxable items.
- l. **Certification Regarding Debarment:** Contractor certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Contractor nor Contractor's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in Federal programs, or programs supported in whole or in part by Federal funds. Contractor further certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, Contractor is not presently debarred, suspended, nor named on the State's debarment list at: <http://bgs.vermont.gov/purchasing/debarment>
- m. **Confidentiality:** Contractor acknowledges and agrees that this Agreement and any and all information obtained by the State from the Party in connection with this Agreement are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq.
- n. **Marketing:** Contractor shall not refer to the State in any publicity materials, information pamphlets, press releases, research reports, advertising, sales promotions, trade shows, or marketing materials or similar communications to third parties except with the prior written consent of the State.
- o. **Non-Appropriation:** If an order made under this Participating Addendum extends into more than one fiscal year of the State (July 1 to June 30), and if appropriations are insufficient to support the order, the State Purchaser may cancel the order at the end of the fiscal year, or otherwise upon the expiration of existing appropriation authority. If the order is funded in whole or in part by Federal funds, and those Federal funds become unavailable or reduced, the State Purchaser may suspend or cancel the order immediately and shall have no obligation to pay from State revenues. State agrees to provide written notice to the Contractor in the event of any suspension or cancellation pursuant to this section.
- p. **Continuity of Performance:** In the event of a dispute between Contractor and the State, each party will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.
- q. **State Facilities:** If the State makes space available to Contractor in any State facility during the term of this Agreement for purposes of Contractor's performance under this Agreement, Contractor shall only use the space in accordance with all policies and procedures governing access to and use of State facilities which shall be made available upon request. State facilities will be made available to Party on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

**Contractor:** CherryRoad Technologies Inc.

By signing below Contractor agrees to offer the products and services on the Master Agreement at prices equal to or lower than the prices listed on the Master Agreement.

**WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT**

By the State of Vermont:

By CherryRoad Technologies Inc.:

Date: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_



## STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 4

CONTRACT #: AR2476

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and CherryRoad Technologies Inc. (Referred to as CONTRACTOR).

### BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

As a result of the Cloud Solutions “refresh” under solicitation # SK18008, Contractor’s master agreement is amended to incorporate Software as a Service (SaaS) into the Agreement’s awarded scope.

- ⌚ Attachment A section 19. Ordering is amended to incorporate the following statement:
  - j. Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order
- ⌚ Attached Exhibit 1 to Master Agreement: Software-as-a-Service is incorporated as an exhibit into Attachment A.
- ⌚ Attached Attachment B Scope of Services Awarded to Contractor replaces the current Attachment B.
- ⌚ Attached Attachment C Pricing Discounts and Pricing Schedule is incorporated into the current Attachment C.

Effective Date of Amendment: 2/1/2019

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

**CONTRACTOR**

**STATE OF UTAH**

Jeremy Gulban

Feb 13, 2019

Christopher Hughes

Feb 13, 2019

Jeremy Gulban (Feb 13, 2019)

Christopher Hughes (Feb 13, 2019)

Contractor’s Signature

Date

Director, State of Utah Division of Purchasing

Date

Jeremy Gulban

Contractor’s Name (Print)

CEO

Title (Print)

### For Division of Purchasing Internal Use

Purchasing Agent	Phone #	E-mail Address	Contract #
Solomon Kingston	801-538-3228	skingston@utah.gov	AR2476

## **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.

## Attachment B – Scope of Services Awarded to Contractor

### **1.1 Awarded Service Model(s).**

Contractor is awarded the following Service Models:

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

Note - CherryRoad is a full-service system integrator with a focus on supporting clients in the public sector in various technology initiatives utilizing IaaS, PaaS, and SaaS solutions. As an Oracle Platinum partner, we provide private cloud services (IaaS and PaaS), ERP systems implementations and upgrades, custom development, and support services that help maximize Oracle's systems' performance.

### **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	
PaaS	x	x	x	
SaaS	x	x	x	

\*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

### 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 a Contractor 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.

### Cloud Service Model: Software as a Service (SaaS)

Description	Discount
SaaS Minimum Discount % (applies to all OEM's offered within this SaaS model)	25.00%
<b>Average SaaS OEM Discount Off</b>	<b>25.00%</b>

### Additional Value Added Services

Item Description	Onsite Hourly Rate		Remote Hourly Rate	
	NVP Price	Catalog Price	NVP Price	Catalog Price
Maintenance Services	n/a	n/a	n/a	n/a
Professional Services				
Deployment Services	See note below	See note below	See note below	See note below
Integration Services)	"	"	"	"
Consulting/Advisory Services	"	"	"	"
Architectural Design Services	"	"	"	"
Statement of Work Services	"	"	"	"
Partner Services	"	"	"	"
Training Deployment Services	"	"	"	"

Please note - the services above are based on the overall project plan, timing, size of the organization etc

### Deliverable Rates

Services Hourly Rates			
Position	Government List Price (\$)	Percent Discount	Hourly Rate (\$)
Program Manager - Onsite	\$644	65%	\$225
Project Manager - Onsite	\$570	65%	\$200
Functional Lead - Onsite	\$528	65%	\$185
Specialty Products Lead - Onsite	\$570	65%	\$200
Technical Lead - Onsite	\$528	65%	\$185
Technical Developer - Onsite	\$415	65%	\$145
Database Administrator - Onsite	\$470	65%	\$165
System Administrator - Onsite	\$470	65%	\$165
Upgrade Specialist - Onsite	\$528	65%	\$185
Change Management Lead - Onsite	\$470	65%	\$165
Training Manager - Onsite	\$528	65%	\$185
Trainer - Onsite	\$470	65%	\$165
Security/Portal Lead - Onsite	\$528	65%	\$185
Oracle Cloud Specialist - Onsite	\$900	65%	\$315
Assessments Specialist - Onsite	\$570	65%	\$200
Program Manager - Offsite	\$558	65%	\$195
Project Manager - Offsite	\$486	65%	\$170
Functional Lead - Offsite	\$444	65%	\$155
Specialty Products Lead - Offsite	\$486	65%	\$170
Technical Lead - Offsite	\$444	65%	\$155
Technical Developer - Offsite	\$315	65%	\$110
Database Administrator - Offsite	\$385	65%	\$135
System Administrator - Offsite	\$385	65%	\$135
Upgrade Specialist - Offsite	\$444	65%	\$155
Change Management Lead - Offsite	\$385	65%	\$135
Training Manager - Offsite	\$444	65%	\$155
Security/Portal Lead - Offsite	\$444	65%	\$155
Oracle Cloud Specialist - Offsite	\$820	65%	\$287

Attachment C - Pricing Discounts and Schedule

Assessments Specialist - Offsite	\$500	65%	\$175
Onsite Rate Includes Travel Expenses			



## STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 3

CONTRACT #: AR2476

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and CherryRoad Technologies Inc. (Referred to as CONTRACTOR).

**BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:**

The Master Agreement AR2476 is amended to include the following cloud solutions products and services in its service offerings.

CONTRACTOR has added new products and service offerings under the cloud solutions portfolio. Oracle is unable to provide CONTRACTOR with discounts on certain new cloud solutions that allow for the originally agreed upon level of discounting to the end customer. Therefore these additional offerings are not discounted in the same manner as those offerings which CONTRACTOR included in the initial proposal. CONTRACTOR is amending its price catalog to reflect a 10 percent discount that is only applicable to new Oracle offerings added after the effective date of this amendment.

Effective Date of Amendment: 11/26/2018

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

STATE OF UTAH

 11-16-2018 Christopher Hughes (Nov 19, 2018) Nov 19, 2018

Contractor's Signature

Date

Director, State of Utah Division of Purchasing

Date

Jeremy Gulban

Contractor's Name (Print)

CEO

Title (Print)

**For Division of Purchasing Internal Use**

Purchasing Agent	Phone #	E-mail Address	Contract #
Solomon Kingston	801-538-3228	skingston@utah.gov	AR2476





## STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 2

CONTRACT #: AR2476

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and CherryRoad Technologies, Inc. (Referred to as CONTRACTOR).

### BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

Section 6 on the master agreement cover page is amended to provide Attachment E as "Service Offering EULAs".

Further, the following End User License Agreement (EULA) attached herein is made a part of Attachment E:

1. DR Fortress Master Services Agreement Terms.

The DR Fortress Master Services Agreement Terms are not to be construed to amend any term or condition provided outside of Attachment E.

Effective Date of Amendment: 2/9/2018

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

STATE OF UTAH

 2/9/18  
Contractor's Signature Date

 2/12/18  
Director, State of Utah Division of Purchasing Date

**Lisa Druckman**  
Contractor's Name (Print) **Vice President Finance**

Title (Print)

### For Division of Purchasing Internal Use

Purchasing Agent	Phone #	E-mail Address	Contract #
Solomon Kingston	801-538-3228	<a href="mailto:skingston@utah.gov">skingston@utah.gov</a>	AR2476



## ATTACHMENT E

### DRFORTRESS, LLC

### MASTER SERVICE AGREEMENT TERMS

THESE MASTER SERVICE AGREEMENT TERMS ("MSA") shall apply to all orders placed under the Master Agreement with DRFortress Technologies Inc. ("DRFortress") for services ultimately provided by DRFortress LLC.

#### 1. ORDERS

Client may request Services during the Term by executing a Sales Order or Order Amendment and delivering the same to DRFortress. Sales Orders and Order Amendments are binding upon DRFortress' execution thereof. DRFortress may reject any Sales Order or Order Amendment and refund the applicable payment for any or no reason. All Sales Orders and Order Amendments and/or any other agreements relating to Services (collectively "Order" or "Orders") are governed by and made a part of this MSA.

#### 2. TERM

Intentionally Omitted.

#### 3. SERVICES AND SERVICE FEES

3.1 DRFortress shall provide Services to Client subject to and in accordance with the provisions of this MSA. Subject to the terms and conditions of this MSA, DRFortress grants Client a limited and non-exclusive license to use the Datacenter and to obtain the Services in accordance with this MSA. Client acknowledges and agrees that (a) it has been granted only a license to use the Datacenter and to obtain the Services in accordance with this MSA; (b) Client has not been granted any real property interest under this MSA; and (c) Client has no rights as a tenant or otherwise under any real property or landlord/tenant laws, regulations or ordinances. This MSA and the rights of Client hereunder, are, without any further action by any Party, subject and subordinate to the leases for the Datacenter and all superior instruments to such leases (including, without limitation, mortgages or ground leases for the Datacenter). DRFortress hereby reserves, with respect to the Datacenter, all rights not specifically granted to Client in this MSA, including without limitation, the right (a) of access to and use of the Datacenter for its own use or the use of others; (b) to grant additional licenses to other entities or clients for the use of portions of the Datacenter and the provision of Services; and (c) to exercise or grant other rights not inconsistent with the rights granted in this MSA. DRFortress shall act as the intermediary for Client with any 3<sup>rd</sup> party building owner or landlord and, where applicable, to reasonably assist in the request of any additional access rights required by Client.

3.2 The Service Fees and Term for any Services ordered through an Order shall be listed on such Order. The Service Fees for the Services shall accrue on each Order Effective Date. Notwithstanding anything in this MSA (or any Order) to the contrary, (a) at any time on or after the expiration of the initial term of the applicable Order, the rates and fees for Services shall be subject to change, at DRFortress' sole discretion, upon 60 days' prior notice to Client, and (b) for the Power Services, DRFortress may change the rates and fees at any time, including the use of a surcharge, upon written notice to Client should the relevant utility increase its effective rate.

3.3 DRFortress shall invoice Client in advance for the Services on a monthly basis (partial months shall be billed on a pro-rata basis). Client shall pay in full all Service Fees, taxes, and surcharges for Services due at the end of each calendar month, or as otherwise indicated on the invoice ("Due Date"). If Service Fees are not paid within 60 days from the Due Date, (a) a late fee of 5% of the overdue amount shall become due and payable by Client, (b) such overdue amount will accrue interest from the Due Date to the date of payment, at an interest rate equal to the lower of 1.5% per month or the highest rate allowed under applicable law, and (c) Client shall reimburse DRFortress for all of its attorneys' fees and costs associated with DRFortress' recovery of Service Fees pursuant to this Section. DRFortress is neither responsible nor is in any way liable for any Taxes or third party charges related to the Client's activities, ownership or operation of equipment at, or attributable to, the Datacenter, including without limitation any activities, ownership, or operation by any of Client's Authorized Persons, Accompanying Persons, and Associated Entities. Without limiting the foregoing, Client shall be responsible for paying any and all Taxes separately imposed, levied or assessed against Client by, and preparing and filing any necessary return from,

any governmental, quasi-governmental or tax authorities by the date such payments and returns are due. All payments to DRFortress are exclusive of all applicable taxes, fees, surcharges, or levies whatsoever, now or in the future imposed on the transaction or the delivery of Services, all of which Client shall pay in full as invoiced by DRFortress. DRFortress may charge for, and client agrees to pay upon invoice, any relevant excise, use, or other transaction related taxes in forms including, but not limited to, a one-time tax charge or as a surcharge spread over a period of time.

3.4 If Client wishes to dispute any charge billed to Client by DRFortress (a "Disputed Amount"), Client must submit a good faith claim regarding the Disputed Amount with supporting documentation within 30 days of receipt of the relevant initial invoice. If Client does not submit a documented claim within 30 days of receipt of the relevant initial invoice, notwithstanding anything in this MSA to the contrary, Client waives all rights to: (a) dispute such Disputed Amount, (b) file a claim thereafter of any kind relating to such Disputed Amount, (c) otherwise claim that it does not owe such Disputed Amount, and/or (d) seek any set-offs or reimbursements or other amounts of any kind based upon or relating to such Disputed Amount. The foregoing notwithstanding, irrespective of whether a documented claim is submitted, Client shall pay all amounts invoiced (including Disputed Amounts) which Disputed Amounts shall be credited against future payments should DRFortress agree that such funds are not due.

#### 4. CLIENT RIGHTS AND OBLIGATIONS

4.1 After obtaining authorization from DRFortress, Client may install Client Equipment in the Space specified for Client, as provided in the Order or as otherwise specified by DRFortress. Client shall be responsible for configuring, providing, placing, installing, upgrading, adding, maintaining, repairing and operating Client Equipment, which actions Client may engage in only to the extent permitted by, and subject to, this MSA. Client represents, warrants and covenants that Client has, and shall continue to have, the legal right and authority (including regulatory consents) to operate, configure, provide, place, install, upgrade, add, maintain and repair Client Equipment as contemplated by this MSA. Without limiting the foregoing, Client shall obtain, and maintain throughout the Term, such consent of Client's subcontractors, 3<sup>rd</sup> party providers, vendors, Sublicensees and any other parties as may be necessary for DRFortress (including any contractors or others acting at DRFortress' request) to have the right to access Client Equipment for the purpose of providing Services. In no event shall Client Equipment be construed to be fixtures. Nothing in the foregoing shall be interpreted as allowing changes (other than to the software) or additions to Client Equipment or environment without DRFortress' approval. Upon request, Client agrees to provide and update DRFortress with estimated market values for the Client Equipment.

4.2 At all times during the Term, DRFortress and Client agree to comply with the Policies, which are at all times incorporated by reference into this MSA. Client acknowledges that it has received a copy of the current Policies prior to execution of this MSA. Any modifications by DRFortress to the Policies shall be effective upon the earlier of: notice to Client or posting on the Client Services Portal. The Space shall only be accessed in accordance with DRFortress' security and access policies and rules. DRFortress shall have the right, but not the obligation, to restrict access to Client's Authorized Persons. Client shall have no license to access, use, operate or store Client Equipment (including, without limitation, conduits and cabling) in any location other than the Space as specified in the Order or as otherwise approved by DRFortress. DRFortress shall have access to the Space in order to perform Services, maintenance or repairs, to make alterations, and to show and inspect the Space. DRFortress may modify or suspend Services as necessary to comply with any law, regulation, the Policies, or as otherwise reasonably determined by DRFortress. Client may use the Space only for purposes of storing, maintaining, and operating Client Equipment in a manner consistent with the business and operations of the Datacenter. Client shall not use the Space for general office use or for any other purpose. Client agrees not to interfere with the use of the Datacenter by other clients, licensees, occupants, or tenants. If Client or any Authorized Person, Accompanying Person or Associated Entities, or the Client Equipment, interferes with the operations of the Datacenter or with any operations or equipment of any other client, licensee, occupant or



tenant of the Datacenter, Client shall promptly eliminate all such interference. If Client is unable or unwilling to eliminate such interference in a reasonable time frame based on the urgency of the circumstances, DRFortress may do so at Client's sole expense. No work or alterations to the Datacenter shall be performed by or on behalf of Client unless approved in writing and in advance by DRFortress, and Client shall not cause any liens to be imposed upon the Datacenter, including any mechanic's lien or similar lien filed by any Authorized Person, Accompanying Person, or Associated Entity. Without limiting the foregoing, in the event any such lien is filed, Client shall be responsible for the immediate satisfaction, payment or bonding of any such lien and any costs incurred by DRFortress in connection therewith.

4.3 If Client is entitled to Interconnection Services under any Order(s), Client shall follow the procedures and rules set forth in this Section and in applicable provisions of the Order(s). Notwithstanding anything to the contrary set forth herein, Client shall not have any right whatsoever to perform Interconnection Services except to the extent otherwise agreed to in writing by DRFortress. All Interconnection Services shall be provisioned exclusively by DRFortress and no Interconnection Services shall be performed in any other manner or location whatsoever, including without limitation wireless Interconnection Services, unless otherwise designated by DRFortress in its sole and absolute discretion. Client acknowledges that DRFortress does not make any representations or warranties regarding Client's ability to establish Interconnection Services with other clients, licensees or tenants in the Datacenter. Client's inability to establish Interconnection Services with other clients, licensees or tenants in the Datacenter shall not affect Client's obligations under this MSA.

#### 4.4 Intentionally Omitted

4.5 In the event DRFortress determines that it is necessary to relocate Client Equipment, DRFortress shall use commercially reasonable efforts to minimize the interference with Client's use of the Services and Client shall cooperate in good faith with DRFortress to facilitate such relocation. DRFortress shall be responsible for any related costs incurred by DRFortress and for Client's reasonable costs for labor performed within the Datacenter directly incurred in connection with such relocation (but not other costs, special or otherwise, incurred by Client). Notwithstanding the foregoing, if such relocation is due to interference of Client Equipment or otherwise required because of Client or its actions, Client shall be responsible for the costs of such relocation, including all costs incurred by DRFortress and Client.

4.6 DRFortress does not warrant or otherwise guarantee the security of Client Equipment or the Datacenter, and Client agrees that DRFortress will not be liable for any inability, failure or mistake in doing so. Client shall provide to the Datacenter Manager any keys or any other means necessary to access such Client Equipment during emergencies.

4.7 Client shall, at its sole cost and expense, promptly (but in any event no later than 5 business days after demand by DRFortress) remove any unused/dead cables in the Space, Datacenter and/or any other portion of the Building (without providing Client the right to have any cabling except to the extent set forth in any Order), and promptly repair all damage resulting from such removal. If Client fails to comply with the foregoing terms of this Section, then DRFortress may, upon 48 hours written notice, remove such unused/dead cables. Moreover, DRFortress may repair those portions of the Datacenter and/or any other portion of the Building damaged by the removal (whether performed by DRFortress, Client, or a 3<sup>rd</sup> party), and Client shall, upon demand, promptly pay to DRFortress all related costs and expenses, including, without limitation, DRFortress' administrative fee of 15% of the cost of such work.

4.8 If Client or any Authorized Person, Accompanying Person, or Associated Entity damages the Datacenter or any equipment contained therein, DRFortress shall have the right and may, in its sole discretion, repair such damage and Client shall, upon demand, promptly pay to DRFortress all costs and expenses incurred in connection therewith, including, without limitation, DRFortress' administrative fee of 15% of the cost of such work.

### 5. CLIENT REPRESENTATIONS

Client represents and warrants that at all times: (a) Client has, and will maintain, the legal right and authority to install and use Client Equipment as contemplated under this MSA, (b) the performance of its obligations under this MSA and use of Services and Client Equipment will not violate applicable manufacturer's specifications, laws regulations, rules, regulations, or policies (including the Policies), or unreasonably interfere with other DRFortress clients' use of Services, or with the use of services provided to any clients, licensees, tenants, or other occupants of the Datacenter or Building, and (c) the individual(s) executing this MSA on behalf of Client, including any Order, is/are authorized to do so.

5.1

### 6. CONFIDENTIAL; INTELLECTUAL PROPERTY

6.1 Except as expressly permitted in this MSA, no Party shall, without the prior written consent of the other Party, disclose any Confidential Information of the other Party to any third party. Information shall be considered Confidential Information of Party if either (a) it is disclosed by the Party to the other Party in tangible form and is conspicuously marked "Confidential", "Proprietary" or the like; or (b)(i) it is disclosed by a Party to the other Party in non-tangible form and is identified as confidential at the time of disclosure; or (ii) it contains the disclosing Party's client/vendor lists, client information, technical information, pricing information, pricing methodologies, information regarding business planning or business operations, or other information that would appear proprietary or confidential to a reasonable person. Notwithstanding anything in this MSA to the contrary, the design of the Datacenter, the Services provided and equipment used at the Datacenter and the configuration, interconnection, switching and routing of telecommunication cables, networks, and services at the Datacenter shall be considered Confidential Information of DRFortress.

6.2 Other than the terms and conditions of this MSA, information shall not be deemed Confidential Information hereunder if such information: (a) is known to the receiving Party prior to receipt from the disclosing Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party, (b) becomes known (independently of disclosure by the disclosing Party) to the receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party, (c) becomes publicly known or otherwise ceases to be a secret or confidential, except through a breach of this MSA or other breach of confidence, or (d) is independently developed by the receiving Party.

6.3 Each Party shall secure and protect the Confidential Information in the same manner it protects its own trade secrets and confidential information, but not using less than a reasonable degree of care. Each Party may disclose the other Party's Confidential Information where (a) the disclosure is required by applicable law or regulation or by an order of a court or other governmental body having jurisdiction after giving reasonable notice to the other party with adequate time for such other Party to seek a protective order; (b) if in the opinion of counsel for such Party, disclosure is advisable under any applicable securities laws regarding public disclosure of business information; or (c) the disclosure is reasonably necessary and is made to that Party's, or its Affiliates', employees, officers, directors, attorneys, accountants and other advisors, or the disclosure is otherwise necessary for a Party to exercise its rights and perform its obligations under this MSA, so long as in all such cases referenced in the clauses above the disclosure is no broader than necessary and the person or entity receiving the disclosure agrees prior to receipt to keep the information confidential. Each Party is responsible for ensuring that any Confidential Information disclosed pursuant to this MSA (other than disclosures pursuant to clauses (a) and (b)) is kept confidential by the person receiving the disclosure to the same extent that the receiving Party must keep the information confidential.

6.4 Notwithstanding the restrictions set forth in this MSA, during the Term: (a) DRFortress may issue a press release announcing Client's entry into the Datacenter without obtaining Client's consent; and (b) either Party may publicly refer to the other Party, orally and in writing, as a client or vendor of services of or to the other Party, as the case may be, without obtaining consent from such other Party.

6.5 Client is and shall remain exclusively entitled to all right, title and interest in and to all of Client's Technology, its Confidential Information and other intellectual property. DRFortress is and shall remain exclusively entitled to all right, title and interest in and to all of DRFortress' Technology, its Confidential Information and other intellectual property. No Party shall, directly or indirectly, reverse engineer, decompile, disassemble or otherwise attempt to derive source code or other trade secrets from the Technology or other property of the other Party.

### 7. NO 3<sup>rd</sup> PARTY BENEFICIARIES; INDEMNIFICATION

7.1 DRFortress and Client agree that there shall be no 3<sup>rd</sup> party beneficiaries to this MSA including, but not limited to, the insurance providers for any Party.

7.2 Client shall indemnify, defend, protect and hold harmless DRFortress, its Affiliates and their respective employees, officers, directors, attorneys, accountants and other advisors (collectively, the "Indemnified Parties"), from and against any and all costs, damages, liabilities, losses, and expenses (including, but not limited to, reasonable attorneys' fees and costs) resulting from any claim, suit, action, or proceeding brought by any third party against any Indemnified Party alleging (a) the infringement or misappropriation of any intellectual property right or other unlawful or illegal wrongdoing by Client relating to the delivery or use of Services by Client, its Associated Entities or their respective officers, directors, principals, employees, agents, assignees and sublicensees; (b) personal or physical injury or damage to tangible property caused by Client or any Authorized Person, Accompanying Person or Associated Entity, or their respective officers, directors, principals, employees, agents, assignees or sublicensees; (c) any work done at the Datacenter by or for Client, or any negligent act or omission by Client or any

Authorized Person, Accompanying Person or Associated Entity, or their respective officers, directors, principals, employees, agents, assignees and sublicensees, or any breach of this MSA by Client; and (d) any damages arising out of the Services or the failure of Services, or the use by Client or its employees, agents, contractors, assignees or sublicensees of the Datacenter, or any claims that Client has failed to fulfill a contractual obligation with a third party, or the destruction of or damage to Client Equipment, except as caused by DRFortress' gross negligence or willful misconduct.

7.3 DRFortress shall indemnify, defend and hold harmless the Client and its Affiliates, owners, officers, directors, employees, and agents of Client or of the Affiliates of Client from any and all liability, damages, costs and expenses (including reasonable attorneys' fees and expenses) for personal injury or damage to tangible property resulting from the gross negligence or willful misconduct of DRFortress.

7.4 Through counsel of its own choosing, an Indemnified Party (including for purposes of this Section a party indemnified under Section 8.3) has the right to participate in (but no control over the defense of) any proceeding in which it is being indemnified under this MSA. In such event the Indemnified Party shall be solely responsible for paying the legal fees and expenses for its own counsel. The indemnifying party shall, however, continue to be solely responsible for all other expenses relating to the action, including the legal fees and expenses of the counsel it selects to defend the claims. The indemnifying party shall not take any action which unreasonably exposes the Indemnified Party to a risk of damages, which would not be covered by such indemnity, and may not settle any matter without the prior written consent of the Indemnified Party, which shall not be unreasonably withheld.

#### **8. WARRANTY DISCLAIMER; LIMITATIONS OF LIABILITY**

8.1 DRFORTRESS DOES NOT WARRANT THAT THE SERVICES PROVIDED HEREUNDER SHALL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE. DRFORTRESS DOES NOT MAKE, AND DRFORTRESS HEREBY DISCLAIMS, ANY AND ALL IMPLIED WARRANTIES WITH REGARD TO THE SERVICES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. EXCEPT AS OTHERWISE EXPRESSLY SET FORTH IN THIS MSA, DRFORTRESS DOES NOT MAKE, AND HEREBY DISCLAIMS, ALL EXPRESS WARRANTIES WITH REGARD TO THE SERVICES. ALL SERVICES PROVIDED PURSUANT TO THIS MSA ARE PROVIDED OR PERFORMED ON AN "AS IS", "AS AVAILABLE" BASIS, AND CLIENT'S USE OF THE SERVICES IS SOLELY AT ITS OWN RISK.

8.2 NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS MSA, IN NO EVENT SHALL DRFORTRESS OR CLIENT BE LIABLE TO THE OTHER PARTY FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, RELIANCE, EXEMPLARY OR PUNITIVE DAMAGES OF ANY NATURE WHATSOEVER, INCLUDING LOST PROFITS, LOSS OF BUSINESS, LOSS OF REVENUES, LOSS OF DATA, INTERFERENCE, INTERRUPTION OR CORRUPTION OR ANY OTHER TYPE OF DAMAGES OTHER THAN DIRECT DAMAGES.

8.3 NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS MSA, DRFORTRESS' TOTAL LIABILITY TO CLIENT IN THE AGGREGATE FOR THE ENTIRE TERM (AND REGARDLESS OF WHETHER THE CLAIMS ARE BROUGHT DURING OR AFTER THE TERM) WITH RESPECT TO ALL CLAIMS ARISING FROM OR RELATED TO THE SUBJECT MATTER OF THIS MSA (INCLUDING ATTORNEYS' FEES) SHALL NOT EXCEED THE AMOUNT ACTUALLY PAID BY CLIENT TO DRFORTRESS FOR THE THREE MONTH PERIOD IMMEDIATELY PRECEDING THE MONTH IN WHICH THE FIRST CLAIM AROSE. AS A FURTHER LIMITATION, DRFORTRESS' MAXIMUM LIABILITY FOR ANY CLAIMS RELATING TO SERVICES OFFERED OR PROVIDED BY DRFORTRESS (A) FOR A NON-RECURRING CHARGE ONLY OR (B) AS REMOTE ASSISTANCE SERVICES, SHALL NOT EXCEED THE AMOUNT OF THE SERVICE FEE FOR SUCH SERVICE PROVIDED ON THE OCCASION GIVING RISE TO THE CLAIM.

8.4 THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY TO ANY AND ALL CLAIMS AND CAUSES OF ACTION WHATSOEVER, REGARDLESS OF WHETHER IN CONTRACT, TORT, STRICT LIABILITY, OR OTHER THEORY.

8.5 DRFortress and Client each waive the right to bring any claim against the other Party arising or in any way relating to this MSA more than one year after the date this MSA expires or is earlier terminated.

8.6 The Parties acknowledge and agree that the disclaimer of warranties and limitations of liability set forth in this Section 9 are essential parts of this MSA and that the Services Fees would be materially higher in the event any portion of such provisions were not enforced in full.

8.7 Notwithstanding anything to the contrary set forth in this MSA or Order, and without limiting any other waivers or limitations set forth in this MSA or Order, Client shall have no termination or abatement rights whatsoever in the event that Client is unable to use or properly utilize any Services as a result of Client's inability to establish Interconnection Services.

#### **9. SUSPENSION; TERMINATION; EXPIRATION; REMEDIES**

9.1 DRFortress may suspend any or all of the Services, including suspending the supply of power and denying access to the Datacenter, if (a) Client fails to cure any monetary breach of this MSA within 10 days of notice of the same (five (5) days in the event Client's account is past due on three (3) or more occasions during a six (6) month period); (b) Client breaches any provision of this MSA that in DRFortress' reasonable judgment interferes with DRFortress' operation or maintenance of a Datacenter or with one or more of its other clients' use thereof, and Client fails to cure such breach within 1 hour of being informed of the same; or (c) Client breaches any provision of this MSA that in DRFortress' reasonable judgment has the potential to interfere with DRFortress' operation or maintenance of a Datacenter or with one or more of its other Clients' use thereof, and Client fails to cure such breach within 48 hours of being informed of the same. If DRFortress suspends a Service pursuant to this Section, unless DRFortress has subsequently terminated this MSA as permitted under this MSA, DRFortress shall resume the discontinued Service within 24 hours after it is reasonably satisfied Client has cured the breach(es) which gave rise to such suspension. DRFortress may charge a reinstatement fee equal to the direct out-of-pocket expenses incurred by DRFortress to discontinue and resume the Service.

9.2 DRFortress may terminate this MSA upon written notice of termination to Client, if (a) Client breaches any material term or condition of this MSA (including, without limitation, the failure to pay Service Fees when due) and, if such breach arises due to a failure to pay Service Fees, such failure continues for 3 business days after such Fees are past due, and, with respect to other breaches (other than as provided in this paragraph as subsections (b) and (c) below), Client fails to cure such breach within 10 days after receipt of written notice of breach from the Party sending the notice; (b) Client files a voluntary petition in bankruptcy or commences any voluntary proceeding relating to insolvency, receivership, liquidation, or composition or assignment for the benefit of its creditors; or (c) Client becomes the subject of an involuntary petition, in bankruptcy or any involuntary proceeding relating to insolvency, receivership, liquidation or composition or assignment for the benefit of creditors if such petition or proceeding is not dismissed within 30 days of filing.

9.3 DRFortress may terminate this MSA, by written notice to Client in the event (a) the Datacenter is wholly or partially damaged by fire, windstorm, tornado, flood or by similar causes or casualties, whether or not the Services are affected, and one or more of the following conditions are present: (i) in DRFortress' reasonable judgment, the repairs cannot be accomplished within 180 days after the date of discovery of the damage, (ii) the holder of any mortgage or deed of trust or a ground lessor requires the insurance proceeds be used for purposes other than the repair, (iii) the damage is not fully covered by DRFortress' insurance, (iv) the damage occurs during the final 12 months of the Term, or (v) the cost to repair exceeds \$500,000 in the aggregate; (b) all or any portion of the Datacenter is taken by power of eminent domain, or DRFortress grants a deed or other instrument in lieu of such taking; or (c) any portion of the Datacenter becomes subject to a condemnation proceeding or is condemned and DRFortress' possession is otherwise terminated or abated or DRFortress cannot provide Client with access to the affected Space as contemplated herein for a period exceeding 30 days. If DRFortress does not terminate this MSA, DRFortress shall have a reasonable time within which to rebuild or make any repairs. Client is responsible to repair and replace any damaged or destroyed Client Equipment. DRFortress shall have no liability to Client for any casualty, eminent domain or failure or suspension of Services, or for any annoyance, inconvenience, injury or damage related to such event or any repairs or restoration.

9.4 Client may terminate this MSA upon written notice of termination to DRFortress, if DRFortress breaches any material term or condition of this MSA and such failure continues for 10 business days after receipt of written notice of breach from the Client.

9.5 Upon the expiration or other termination of this MSA (collectively the "Termination Date"), Client shall remove from the Datacenter all Client Equipment and shall return the Space to DRFortress in the same condition it was provided on the Commencement Date, normal wear and tear excepted, pursuant to a time schedule agreed upon by DRFortress and Client, or if no schedule is agreed upon, within 10 days after the Termination Date. Client shall not, however in DRFortress' sole discretion, be permitted to remove any Client Equipment or retrieve any stored data unless payment of all Service Fees and other amounts due to DRFortress are current and not in default. If Client fails to comply with this paragraph, Client shall be responsible for all damages and costs incurred by DRFortress, and during any period of holdover, and shall also pay DRFortress monthly Service Fees equal to 200% of the monthly Service Fees in effect immediately preceding such holdover.

9.6 If Client does not remove the Client Equipment as required by this MSA, whether or not due to its own past current payment(s) or default, DRFortress may remove Client Equipment to a DRFortress or 3<sup>rd</sup> Party storage area, at Client's expense. DRFortress shall not be liable for any loss or damage caused to Client or its Client Equipment or other property resulting from such removal and storage.

9.7 While neither Party shall be liable to the other for properly terminating this MSA or any portion thereof in accordance with its terms, Client shall be liable to DRFortress for any amounts owed prior to the Termination Date. Notwithstanding anything to the contrary in this MSA, DRFortress has the right to recover from Client all damages recoverable under law or pursuant to this MSA for the period past the end of the Term, if DRFortress terminates this MSA prior to the end of the full Term due to Client's material breach.

9.8 The terms and conditions set forth in this Section 10.8, as well as Sections 3.5, 7, 8.1, 8.2, 8.4, 9, 10.5, 10.6, 10.7, 10.9, 10.10, 12 and 14, and any other terms that by their nature are intended to survive, shall survive the expiration or other termination of this MSA.

9.9 Notwithstanding anything in this MSA or its Orders to the contrary, under no circumstances shall any Order survive the termination of this MSA. DRFortress shall not have any obligation to provide any Services after the expiration or earlier termination of this MSA.

9.10 If DRFortress terminates this MSA because of any reasons set forth in Section 10.2, or if Client terminates this MSA (including any Order) for any reason other than pursuant to Sections 10.3 or 10.4, since the contract damages suffered by DRFortress would be extremely difficult to determine, Client agrees to pay to DRFortress, within 10 days of such termination, an amount equal to 100% of the Service Fees payable for all of the months remaining on the Term of this MSA, as liquidated damages and not as a penalty. These damages shall be in addition to the amounts otherwise then due and payable to DRFortress.

#### 10. SUBLICENSING

10.1 With DRFortress' written consent, not to be unreasonably withheld, Client may sublicense the Space to Sublicensees provided that the following conditions are met: (a) the terms and conditions of such sublicense shall be no less restrictive than this MSA; (b) Client shall not in its dealing with such Sublicensees act or purport to act on behalf of DRFortress or landlord(s) of DRFortress; (c) Client shall require the Sublicensees to abide by the rules set forth in the Policies; (d) the agreement between Client and Sublicensee shall provide that Sublicensee has no right to sublicense, delegate, assign or otherwise transfer its rights to use the Sublicensed Space to any other person or entity without DRFortress' written consent, which consent may be withheld for any reason whatsoever or no reason, and without such consent any such sublicense, delegation, assignment or transfer shall be null and void; and (e) Client shall cause all Sublicensees to agree in writing that in consideration for the sublicense, Sublicensees waive, to the maximum extent permitted under law, any and all claims of any and all types against DRFortress and the landlord(s) of DRFortress, at all times, and that in no event shall DRFortress, or the landlord(s) of DRFortress have any liability to such Sublicensees, including liability to such Sublicensees for any damages whatsoever, including direct damages.

10.2 Notwithstanding anything in this MSA to the contrary, Client shall remain responsible to DRFortress for the performance of all of Client's obligations under this MSA and all other agreements between DRFortress and Client. No sublicense agreement or arrangement between Client and any Sublicensees shall relieve Client from any liability under this MSA. Without limiting the foregoing, Client is responsible for paying the Service Fees for all of the Space (including Sublicensed Space) and the charges for Services for, or relating to, any or all of the Space (including Sublicensed Space). In no event shall DRFortress be deemed to be providing any Services to any Sublicensee for, or relating to, the Sublicensed Space, as the provision of any such Services shall be deemed to be to Client for all purposes under this MSA. In addition, notwithstanding anything in this MSA to the contrary, under no circumstances shall DRFortress be deemed to have any obligations to any Sublicensee. Client must ensure that each and every sublicense agreement or other sublicense arrangement that Client has with a Sublicensee does not have any terms and conditions that (i) are inconsistent with this MSA, or (ii) seek to provide any Sublicensee with rights that Client does not have under this MSA. Without limiting the foregoing or any other restrictions on Sublicensees, no Sublicensee shall have any right to use its Sublicensed Space in any manner that Client is not permitted to use the Space, and Client shall ensure that its agreement with each Sublicensee shall clearly indicate that Sublicensee does not have any right to use its Sublicensed Space in any manner that Client is not permitted to use the Space.

10.3 Sublicensees do not have any rights, separate and apart from Client's rights, to access their Sublicensed Space. Accordingly, only Client's Authorized Persons at the Datacenter may access the Sublicensed Space of Sublicensees. Furthermore, DRFortress is not responsible for restricting a Sublicensee's access to Client's Space located in a cage or suite to which that Sublicensee has access.

#### 11. DEFINITIONS

11.1 "**Accompanying Person**" means each person (other than an employee of DRFortress) who is accompanied by an Authorized Person while at the Datacenter.

11.2 "**Affiliate**" means as to a Party, means any entity controlling, controlled by, or under common control with such party, where the term "control" and its correlative meanings, "controlling," "controlled by," and "under common control with," means the legal, beneficial or equitable ownership, directly or indirectly, of more than 50% of the aggregate of all voting equity interests in an entity. Without limiting the foregoing, but in addition thereto, any Affiliate of, or subsidiary of, DRFortress, Inc. shall be deemed to be an Affiliate of DRFortress.

11.3 "**Associated Entity**" means each individual, company, partnership or other entity of any type which employs, contracts with, or is otherwise associated or affiliated with any of Client's Authorized Persons or Accompanying Persons. Without limiting the foregoing definition, each Sublicensee that has sublicensed Sublicensed Space at the Datacenter shall be an Associated Entity of the Client.

11.4 "**Authorized Person**" means each person who is then included on the most recent list of Authorized Persons given to DRFortress by Client in accordance with the Policies.

11.5 "**Building**" means the facilities, building or set of buildings within which the Datacenter is located, including portions of such facilities with other tenants.

11.6 "**Client Equipment**" means the Client's computer and network hardware (not including stored data) and all other tangible equipment placed by or on behalf of Client in the Space. The Client Equipment shall be identified on a list delivered by Client to DRFortress, as amended in writing from time to time by Client.

11.7 "**Client Services Portal**" means the website [www.csp.drfortress.com](http://www.csp.drfortress.com) by which Clients can order Supplemental Services for the Space.

11.8 "**Confidential Information**" means any information disclosed by any Party to the other Parties, directly or indirectly, in writing, orally or by inspection of tangible objects that is designated as "Confidential," "Proprietary" or some other similar designation, including information disclosed to a disclosing party by third parties.

11.9 "**Datacenter Manager**" means the DRFortress supervisor with operations authority, whether onsite or on-call, for the Datacenter.

11.10 "**Datacenter Services**" means all services other than the Supplemental Services set forth in the Order, as applicable, including without limitation (to the extent set forth in the applicable Order, as applicable) providing Space for the Client Equipment at the Datacenter.

11.11 "**Datacenter**" means the co-location facility operated by DRFortress and located at the address set forth in the Order.

11.12 "**Force Majeure Event**" is any cause beyond a Party's reasonable control, including, without limitation, acts of war, acts of God, earthquake, hurricanes, flood, fire or other similar casualty, embargo, riot, sabotage, labor shortage or dispute, cut communication line, governmental act, insurrections, epidemics, quarantines, inability to procure materials or transportation facilities, failure of power, restrictive governmental laws or regulations, condemnation, failure of the Internet or other reason of a like nature not resulting from the actions or inactions of a Party.

11.13 "**Interconnection Services**" means a physical or wireless interconnection, including cable, connections, and other wiring between computers, servers and other hardware within the Datacenter that (a) connects Client to another DRFortress client, (b) interconnects Client Equipment across multiple Spaces, or (c) interconnects Client Equipment and equipment that is provided by DRFortress.

11.14 "**Online Order**" means an order for Services placed by Client via the Client Services Portal and accepted by DRFortress pursuant to DRFortress' then current ordering procedures (as well as any amendment to such order reflected in an Order Amendment agreed to by the Parties in accordance with the terms of the applicable original Order, Order Amendment and this MSA). Online Orders for additional Services shall be deemed accepted upon DRFortress' providing such Services. Any reduction in the scope of Services or Service Fees shall not be deemed accepted without an Order Amendment or Order Confirmation.

11.15 "**Order**" means any Sales Order, Online Order or Phone Orders, including any modifications to the foregoing pursuant to an Order Amendment or Order Confirmation or otherwise allowed under this MSA.

11.16 "**Order Amendment**" means any written mutually agreed upon addendum or amendment to an Order executed by DRFortress and Client, setting forth additional Datacenter Services and/or the Supplemental Services to be provided to Client by DRFortress, including any Service Fees associated therewith, or otherwise amending any provision of an Order. Any Order Amendment executed by DRFortress and Client in connection with this MSA shall be deemed a part of this MSA, including, without limitation, any additional obligations set forth therein. Any Order Amendment executed by DRFortress and Client in connection with this MSA shall be read together with this MSA to avoid inconsistent interpretations. However, in the event of irreconcilable conflicts between the terms of this MSA and the terms of any Order Amendment, the terms of this MSA shall control. The term of service for any Services specified on the applicable Order Amendment shall commence and terminate on the date(s) set forth in the Order Amendment. If no termination date is set forth in the Order Amendment for



a particular Service, then the termination date shall be the earlier of the expiration or earlier termination of this MSA. With respect to a Service not being provided on a continuous basis, the term for that Service shall terminate on the date the DRFortress Service is no longer provided, at DRFortress' option, in its sole and absolute discretion. All obligations, duties and liabilities of Client under this MSA shall fully apply to all matters set forth in all Order Amendments.

11.17 "**Order Confirmation**" means a document, which may include an electronic mail message, that confirms, among other things, the Services, the quantity of such Services, and the prices of such Services, ordered in an Online Order or Phone Order and which is issued by DRFortress and returned to DRFortress pursuant to the instructions set forth in such document. Not all Online Orders or Phone Orders require Order Confirmations.

11.18 "**Order Effective Date**" means, with respect to any Services, the date DRFortress will begin providing such Services to Client, as indicated on the relevant Order. The Order Effective Date of this MSA shall be the first Order Effective Date of any Services provided to Client hereunder.

11.19 "**Party(ies)**" means the party or parties signing this MSA.

11.20 "**Phone Orders**" means an order for Services placed by Client via telephone and accepted by DRFortress pursuant to DRFortress' then current ordering procedures (as well as any amendment to such order reflected in an Order Amendment agreed to by the Parties in accordance with the terms of the applicable original Order, Order Amendment and this MSA).

11.21 "**Policies**" means the procedures, rules, regulations, security practices and policies adopted by DRFortress that are then in effect for the Datacenter, as they may be amended from time to time by DRFortress. DRFortress may post the Policies on the Client Services Portal as a convenience to the Client. Any Policies posted on the Client Services Portal shall be the Policies then in effect whether or not the Client is given notice of such posting or any changes thereto.

11.22 "**Power Services**" means power circuits for AC and/or DC electrical power ordered by Client. For the avoidance of doubt, Power Services do not include power provided by DRFortress as part of a bundled service.

11.23 "**Remote Assistance Services**" means work, undertaken by DRFortress and billable to Client, as reasonably directed by Client, to provide support to Client Equipment, Space or Services; or, as reasonably determined by DRFortress, to comply with Policies. DRFortress, in its sole and absolute discretion, may accept or reject all or any portion of each request for Remote Assistance Services.

11.24 "**Sales Orders**" means the written (electronic or hardcopy) work order form or forms, executed by both DRFortress and Client, setting forth the scope and Service Fees for a Service to be provided to Client by DRFortress. Client represents, warrants and covenants that any person completing and/or submitting and/or executing any Sales Orders on behalf of Client (including but not limited to via the Client Resource Center), has the unconditional authority to execute the Sales Orders on Client's behalf and that, upon such execution, the Sales Orders will be binding against Client, regardless of whether the person in question has actual, apparent or other authority and Client hereby agrees that it shall be unconditionally prohibited and estopped from asserting otherwise, at any time. Sales Orders executed by both DRFortress and Client in connection with this MSA shall be deemed a part of this MSA, including, without limitation, any additional obligations set forth therein. Any Sales Orders executed by DRFortress and Client in connection with this MSA shall be read together with the MSA and any Order Amendment thereto to avoid inconsistent interpretations. However, in the event of irreconcilable conflicts between the terms of a Sales Order and/or this MSA or the terms of any Order Amendment, the terms of this MSA and/or the Order Amendment shall control. Unless specifically stated to the contrary in any applicable Order Amendment or this MSA, the term of service for a particular Service shall commence and terminate on the date(s) set forth in the Sales Orders as set forth explicitly or determined based on the stated term. If no termination date determinable based on the Sales Orders or any applicable Order Amendment for a particular DRFortress Service, then the termination date shall be the earlier of the expiration or earlier termination of this MSA. With respect to a Service not being provided on a continuous basis, the term for that Service shall terminate on the date the DRFortress Service is no longer provided, at DRFortress' option, in its sole and absolute discretion. In the event that DRFortress continues to provide a Service after the termination date determined by the applicable Sales Orders, the applicable Service shall be provided on a month-to-month basis at DRFortress' then-current rates, as determined by DRFortress in its sole discretion, and in accordance with all other terms and conditions of this MSA, the Sales Order or any Order Amendments thereto. All obligations, duties and liabilities of Client under this MSA shall fully apply to all matters set forth in all Sales Orders.

11.25 "**Service Fees**" means charges for Services as identified in the applicable Order, as applicable. Certain Services may accrue one-time, non-recurring charges and/or monthly recurring charges that recur regularly during the life of the Term.

11.26 "**Services**" means the Datacenter Services, Supplemental Services and any other services provided by DRFortress to Client pursuant to this MSA.

11.27 "**Space**" means that licensed portion or portions of the Datacenter made available to Client as specified in an Order, as applicable.

11.28 "**Sublicensed Space**" means the portion of the Space sublicensed to a Sublicensee by Client pursuant to the terms of this MSA.

11.29 "**Sublicensee**" means a client of Client or other third party who sublicenses all or part of the Space from Client pursuant to this MSA.

11.30 "**Supplemental Services**" means all services other than the Datacenter Services set forth in the applicable Order, including, without limitation (to the extent set forth in the applicable Order): (a) Interconnection Services; (b) Power Services; and (c) Remote Assistance Services.

11.31 "**Technology**" with respect to any Party means such Party's proprietary technology, including (with respect to DRFortress) Services, software tools, hardware designs, algorithms, software (in source and object forms), user interface designs, architecture, class libraries, objects and documentation (both printed and electronic), network designs, know-how, business methods, and any related intellectual property rights throughout the world (whether owned by such Party or licensed to such Party from a third party) and also including any derivatives, improvements, enhancements or extensions of Technology conceived, reduced to practice, or developed by such Party or a related party during the Term.

11.32 "**Term**" means the period or period of time, as set forth in this MSA and/or an Order, during which DRFortress and Client are obligated to perform under this MSA.

## 12. MISCELLANEOUS PROVISIONS

12.1 "**Force Majeure; Court Order; Cancellation**. No Party will be liable for any failure or delay in its performance under this MSA, other than its obligation to make a payment of money under this MSA due to a Force Majeure Event, provided that the non-performing Party: (a) gives the other Party prompt written notice of such cause, and (b) takes all reasonable steps to promptly correct such failure or delay in performance. Neither DRFortress nor Client shall be liable for its failure or delay in its performance under this MSA if such failure or delay is in compliance with and pursuant to an order issued by a court (or other tribunal) of competent jurisdiction. If DRFortress is unable to provide applicable Services for a period in excess of 30 consecutive days for any reason set forth in this section, any Party may cancel this MSA upon written notice, and all Parties shall be released from all liability accruing under this MSA on and after the effective date of such cancellation.

12.2 "**Governing Law; Dispute Resolution**. Intentionally Omitted.

12.3 Intentionally Omitted

12.4 "**Severability; Waiver**. In the event any provision of this MSA is held by a tribunal of competent jurisdiction to be contrary to any law or regulation, the remaining provisions of this MSA will remain in full force and effect. The Parties shall not be deemed to waive any of their rights or remedies under this MSA unless such waiver is in writing and signed by the Party to be bound. The waiver of any breach or default of this MSA shall not constitute a waiver of any subsequent breach or default.

12.5 "**Assignment**. The rights accorded Client under this MSA, or under any Orders, are personal to Client and except as expressly set forth herein may not be assigned, sublicensed, or otherwise transferred (each a "**Transfer**") in any fashion, regardless of whether such an arrangement is characterized as an assignment, a sublicense, a co-location agreement or any other agreement, without the prior written consent of DRFortress, which consent shall not be unreasonably withheld. DRFortress may assign this MSA and/or delegate its obligations under this MSA in whole or in part without obtaining the consent of Client or any other party.

12.6 "**Notice**. Any notice or communication required or permitted to be given under this MSA may be delivered by hand, sent by overnight courier, at the addresses set forth in the most recent Sales Order or at such other address as may hereafter be furnished. Such notice will be deemed to have been given as of the date it is delivered unless such date is a weekend or holiday, in which event such notice will be deemed delivered on the next succeeding business day.

12.7 "**Relationship of Parties**. DRFortress and Client are independent contractors and this MSA (including all Orders) will not establish any relationship of partnership, joint venture, employment, franchise or agency between DRFortress and Client.

12.8 "**Director, Officer and Employee Liability**. Unless otherwise provided in writing, no Party's directors, officers or employees shall have any personal liability to any other Party with respect to this MSA. Except as may be specifically otherwise consented to in writing by an Affiliate of a Party (and none of the other terms of this MSA shall be deemed to constitute such consent), no Party's Affiliates shall have any liability to any other Party with respect to this MSA, including with respect to any Orders.

12.9 "**Entire MSA; Counterparts**. This MSA (including all Orders) constitutes the complete and exclusive agreement between the Parties with respect to the subject matter hereof, and supersedes and replaces any and all prior or contemporaneous discussions, negotiations, understandings and agreements, written and oral, regarding such subject matter. This MSA (including all Orders) may be executed in counterparts.

12.10 **Language.** If this MSA is translated into another language, the translation is for the convenience of the Client and the provisions of the version of this MSA (including all Orders) set forth in English shall prevail for all purposes.

12.11 **Headings.** Headings used in this MSA are for reference only.

12.12 **Binding Effect.** This MSA will bind and inure to the benefit of each Party and each Party's successors and permitted assigns.

12.13 **Delivery of Certificate.** Client shall, at any time and from time to time, upon not less than 10 days' prior written notice from DRFortress, execute, acknowledge and deliver to DRFortress a statement in writing certifying the following information, (but not limited to the following information in the event further information is requested by DRFortress): (a) that this MSA (including all Orders) is unmodified and in full force and effect (or, if modified, stating the nature of such modification and certifying that this MSA (including all Orders), as modified, is in full force and effect); (b) the dates to which the rental and other charges are paid in advance, if any; (c) the amount of Client's security deposit, if

any; and (d) acknowledging that there are not, to Client's knowledge, any uncured defaults on the part of DRFortress under this MSA (including all Orders), and no events or conditions then in existence which, with the passage of time or notice or both, would constitute a default on the part of DRFortress under this MSA (including all Orders), or specifying such defaults, events or conditions, if any are claimed. It is expressly understood and agreed that any such statement may be relied upon by any prospective purchaser or encumbrancer of all or any portion of the Datacenter and/or Building. DRFortress shall prepare a draft of such statement at its sole expense and deliver such draft to Client at the time of its written notice requesting the statement from Client. Client's failure to deliver such statement within such 10 day period shall constitute an admission by Client that all statements contained therein are true and correct. Additionally, Client's failure to deliver such statement within such 10 day period shall constitute a material breach and default by Client under this MSA.



## STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 1

CONTRACT #: AR2476

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and CherryRoad Technologies Inc. (Referred to as CONTRACTOR).

### BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

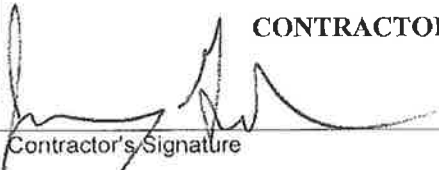
Exhibit 1 was inadvertently left out of the Master Agreement. This amendment adds Exhibit 1 to the Master Agreement. All other existing terms and conditions in the Master Agreement remain in full force and effect.

Effective Date of Amendment: 10/14/2016

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.  
IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

**CONTRACTOR**

**STATE OF UTAH**

  
Contractor's Signature

12/2/16  
Date

  
Kent Beers, Director  
State of Utah Division of Purchasing

10.4.2016  
Date

Jeremy Gulban  
Contractor's Name (Print)

President  
Title (Print)

Purchasing Agent

Phone #

e-mail

Contract #

Spencer Hall

801-538-3307

spencerh@utah.gov

AR2476



## **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 its 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.

Contract # AR2476**STATE OF UTAH COOPERATIVE CONTRACT**

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

CherryRoad Technologies Inc.

Name

301 Gibraltar Drive, Suite 2C

Address

Morris Plains

NJ

07950

City

State

Zip

**LEGAL STATUS OF CONTRACTOR**

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

Contact Person Jeremy Gulban Phone /(973) 402-7802 Email JGulban@cherryroad.comVendor #VC205717 Commodity Code #920-05

2. **GENERAL PURPOSE OF CONTRACT:** Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed
3. **PROCUREMENT PROCESS:** This contract is entered into as a result of the procurement process on Bid#CH16012.
4. **CONTRACT PERIOD:** Effective Date: 09/30/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.
5. **Administrative Fee,** as described in the Solicitation and Attachment A: 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.
6. **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 Pricing Schedule  
**ATTACHMENT D:** Contractor's Response to Solicitation #CH16012  
**ATTACHMENT E:**

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

8. **DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:**  
a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.  
b. Utah State Procurement Code and the Procurement Rules.
9. *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.

**CONTRACTOR**

Contractor's signature

Date

**STATE**

Director Division of Purchasing

Date

Jeremy Gulban, President

Type or Print Name and Title

Christopher Hughes

Division of Purchasing Contact Person

801-538-3254

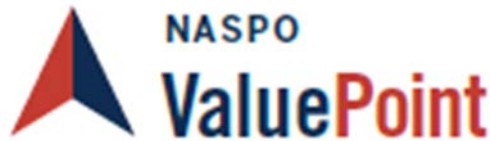
Telephone Number

Fax Number

christopherhughes@utah.gov

Email

(Revision 16 June 2016)



## **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<sup>1</sup> ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits<sup>2</sup> 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 or the Purchasing Entity's or Purchasing Entity's clients in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's or Contractor records, (2) personnel or financial 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.

---

<sup>1</sup> A Sample Participating Addendum will be published after the contracts have been awarded.

<sup>2</sup> The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and SaaS.



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

**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 provided by Contractor under this Master Agreement, including Services, software, and any incidental tangible goods as set forth in a Statement of Work.

**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:** The initial term of this Master Agreement is for ten (10) years with no renewal options.

**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, which written consent to assign, sell, transfer, or sublet rights, or delegate responsibilities under the Master Agreement, in whole or in part shall not be unreasonably withheld.

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, Non-Solicitation, Limitation of Liability and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to either party's default shall be in accordance with Section 10. Contractor shall be paid for all services performed through the date of termination.

**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. Purchasing Entity's or Purchasing Entity's clients acknowledge 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 Contractor. 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 the disclosing party to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in the receiving party's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than the disclosing party without the obligation of confidentiality, (5) is disclosed with the written consent of the disclosing party or; (6) is independently developed by employees, agents or subcontractors of the receiving party who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Unless required by law or legal process, Contractor and Purchasing Entity's or Purchasing Entity's clients shall hold the other party's 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 the other party's 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, Purchasing Entity and Purchasing Entity's clients shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor, Purchasing Entity and Purchasing Entity's clients shall use commercially reasonable efforts to assist in identifying and preventing any unauthorized use or disclosure of any of the other party's 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 the disclosing party, the receiving party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement or required by law or legal process, 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. The parties acknowledge that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury that is inadequately compensable in damages. Accordingly, the non-breaching party 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. The parties acknowledge and agree that the covenants contained herein are necessary for the protection of the legitimate business interests 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 and Contractor had knowledge hereof or should have reasonably known; 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, the non-breaching party shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which the breaching party 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 reasonable 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 the non-breaching party's liability for damages.

c. If the breaching party is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, the breaching party shall be in breach of its obligations under this Master Agreement and non-breaching party 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 only of the amount in dispute until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, Contractor and 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 Lead States approval to changes in key personnel may not be unreasonably withheld. 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, from third party actions, for any death, injury, or damage to property arising directly or indirectly from negligent act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors, 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 by a third party 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 acts or omissions of the Indemnified Party including, without limitation, materials, specifications, or products provided by the Indemnified Party; modifications made by the Indemnified Party to the Products delivered by Contractor; if the Indemnified Party uses the Product in a manner not intended by Contractor; or 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 immediately 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 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 reasonable 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 Purchasing Entity will not be responsible for any deductible in the event of a claim. The minimum acceptable limits shall be as indicated below:

(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	<b>Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions</b>
	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 claim and in the aggregate, written on a claims made basis 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. Purchasing Entities will notify Contractor of any loss of funding. Purchasing Entity will be responsible for payment for all Services performed prior to the termination of the Services.

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 as long as the Order incorporates the terms of the Master Agreement. 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<sup>3</sup>.

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. 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 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

---

<sup>3</sup> 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.

subsection must be consistent with license rights granted for use of intellectual property.

**21. Payment:** 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, upon reasonable notice, 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 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. If the system failure is related to software deficiencies or any inappropriate, improper or unforeseen usage of the work or services by the Purchasing Entity then Contractor will not be responsible for any associated remediation cost.

**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.

Contractor shall retain all right, title, and interest in and to all intellectual property rights embodied in all materials, Contractor's proprietary information, and Contractor Technology in connection with the Services and/or this Agreement. "Contractor Technology" shall mean Contractor's proprietary technology, including but not limited to, Contractor's Services, internet operations design, content, software tools, hardware designs, algorithms, software created by Contractor (in source and object forms), user interface designs, architecture products, user manuals (whether in print or electronic), network designs, know-how, trade secrets, and any related intellectual property rights worldwide (whether owned by Contractor or licensed to Contractor from a third party) and also including any derivative works, improvements, modifications, enhancements, or extensions of Contractor Technology conceived, reduced to practice, or developed prior to or during the term of this Master Agreement or any Order or PA.

**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 it will use commercially reasonable efforts to ensure that the Services 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.

THE WARRANTIES CONTAINED HEREIN AND IN THE STATEMENT OF WORK ARE CONTRACTOR'S SOLE AND EXCLUSIVE WARRANTIES. CONTRACTOR AFFIRMATIVELY EXCLUDES ANY AND ALL OTHER WARRANTIES, CONDITIONS, OR REPRESENTATIONS (EXPRESS OR IMPLIED, ORAL OR WRITTEN), WITH RESPECT TO THE SERVICES PROVIDED INCLUDING ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS OF TITLE, MERCHANTABILITY, OR FITNESS OR SUITABILITY FOR ANY PURPOSE (WHETHER OR NOT THE CONTRACTOR KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR IS OTHERWISE IN FACT AWARE OF ANY SUCH PURPOSE) WHETHER ARISING BY LAW OR BY REASON OF CUSTOM OF THE TRADE.

### **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, Purchasing Entity, or Contractor 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 Purchasing Entity or Contractor must be in writing. Waiver by the Lead State, Participating Entity or Contractor 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 SciQuest, Inc. whereby SciQuest 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://www.naspo.org/WNCPO/Calculator.aspx>. 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 F.

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. 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.

**44. Limitation of Liability:** Except as otherwise set forth in the Indemnification Paragraphs above, the limit of liability shall be as follows :a. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) five million dollars (\$5,000,000), whichever is greater.

b. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

c. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

The limitations of liability will not apply to claims for bodily injury or death, Section 8, Section 13, and Section 30.



## **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) terminate 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, upon reasonable request, 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, upon reasonable request, 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

CherryRoad is a full-service system integrator with a focus on supporting clients in the public sector in various Oracle technology initiatives. As an Oracle Platinum partner, we provide private cloud services (IaaS and PaaS), ERP systems implementations and upgrades, custom development, and support services that help maximize Oracle's systems' performance.



**Proposal for an NASPO ValuePoint Cloud Solutions for the  
State of Utah**

**Solicitation CH16012**

March 10, 2016

**COST PROPOSAL**



# Table of Contents

9. Cost Proposal ..... 1





## 9. Cost Proposal

*Cost Proposals will be evaluated independently from the technical proposal. Offeror's cost proposal must include the items discussed in Section 9 of the RFP.*

*Cost will be evaluated independently from the Mandatory Minimum Requirements, and the Technical responses. Inclusion of any cost or pricing data within the Detailed Technical Proposal will result in the proposal being judged as non-responsive for violation of UCA § 63G-6a-707(5).*

*All costs incurred by an Offeror in the preparation and submission of a proposal, including any costs incurred during interviews, oral presentations, and/or product demonstrations are the responsibility of the Offeror and will not be reimbursed by the Lead State or NASPO ValuePoint.*

Please see:

- **Cost Proposal – CH16012 Cloud Solutions.xlsx**

All pricing reflects a 65% discount off of our government list pricing.

CherryRoad has provided cost tabs for IaaS and PaaS. Tabs for Storage, Network and Disaster Recovery provide additional pricing add on products for both PaaS and IaaS.

Tab 8.21 Secure Authentication reflects Related Value Added Services to the Cloud "Single Sign on, Secure Access and Authentication Platform."

Rate card tab provides both on site and off site rates. On site rates are all inclusive.

# IAAS

Operating System	Description	Memory Class	Memory Qty (# GB)	CPU Core Class	CPU Core Qty (#)	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)
Linux	Oracle Linux on Intel (64-bit)			Small	2	Month	\$97	65%	\$59
Linux	Oracle Linux on Intel (64-bit)			Medium	4	Month	\$162	65%	\$98
Linux	Oracle Linux on Intel (64-bit)			Large	8	Month	\$290	65%	\$176
Linux	Oracle Linux on Intel (64-bit)			XLarge	12	Month	\$256	65%	\$155
Linux	Oracle Linux on Intel (64-bit)			XXLarge	16	Month	\$549	65%	\$333
Linux	Additional Core			Additional	1	Month	\$54	65%	\$33
Windows	Windows 2012 Datacenter (64-bit)			Small	2	Month	\$135	65%	\$82
Windows	Windows 2012 Datacenter (64-bit)			Medium	4	Month	\$236	65%	\$143
Windows	Windows 2012 Datacenter (64-bit)			Large	8	Month	\$439	65%	\$266
Windows	Windows 2012 Datacenter (64-bit)			XLarge	12	Month	\$648	65%	\$393
Windows	Windows 2012 Datacenter (64-bit)			XXLarge	16	Month	\$853	65%	\$517
Windows	Additional Core			Additional	1	Month	\$73	65%	\$45
Linux	Oracle Linux on Intel (64-bit)	Small	4			Month	\$31	65%	\$19
Linux	Oracle Linux on Intel (64-bit)	Medium	8			Month	\$59	65%	\$36
Linux	Oracle Linux on Intel (64-bit)	Large	12			Month	\$86	65%	\$52
Linux	Oracle Linux on Intel (64-bit)	XLarge	16			Month	\$112	65%	\$68
Linux	Oracle Linux on Intel (64-bit)	XXLarge	24			Month	\$167	65%	\$101
Linux	Additional RAM	Additional	1			Month	\$8	65%	\$5
Windows	Windows 2012 Datacenter (64-bit)	Small	4			Month	\$31	65%	\$19
Windows	Windows 2012 Datacenter (64-bit)	Medium	8			Month	\$59	65%	\$36
Windows	Windows 2012 Datacenter (64-bit)	Large	12			Month	\$86	65%	\$52
Windows	Windows 2012 Datacenter (64-bit)	XLarge	16			Month	\$112	65%	\$68
Windows	Windows 2012 Datacenter (64-bit)	XXLarge	24			Month	\$167	65%	\$101
Windows	Additional RAM	Additional	1			Month	\$8	65%	\$5

PAAS

Platform	Description	Memory Class	Memory Qty (# GB)	CPU Core Class	CPU Core Qty (#)	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 16G RAM/1TB Storage)			XSmall	1	Month	\$3,446	65%	\$2,089
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only -32G RAM/2TB Storage)			Small	4	Month	\$13,786	65%	\$8,355
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only -48G RAM/3TB Storage)			Medium	8	Month	\$27,572	65%	\$16,710
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 64G RAM/4TB Storage)			Large	12	Month	\$41,357	65%	\$25,065
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 96G RAM/5TB Storage)			XLarge	24	Month	\$82,715	65%	\$50,130
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 128G RAM/6TB Storage)			XXLarge	32	Month	\$110,286	65%	\$66,840
Exadata	Additional Dedicated Exadata Core (Hardware only - 16GB RAM/1TB Storage)			Additional	1	Month	\$4,125	65%	\$2,500
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			XSmall	1	Month	\$3,446	65%	\$2,089
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			Small	4	Month	\$13,786	65%	\$8,355
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			Medium	8	Month	\$27,572	65%	\$16,710
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			Large	12	Month	\$41,357	65%	\$25,065
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			XLarge	24	Month	\$82,715	65%	\$50,130
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			XXLarge	32	Month	\$110,286	65%	\$66,840
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 4G RAM/300GB Storage)	XSmall	4			Month	\$307	65%	\$186
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 6G RAM/450GB Storage)	Small	6			Month	\$461	65%	\$279
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 8G RAM/600GB Storage)	Medium	8			Month	\$614	65%	\$372
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 12G RAM/900GB Storage)	Large	12			Month	\$922	65%	\$559
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 24G RAM/1.2TB Storage)	XLarge	16			Month	\$1,229	65%	\$745
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 32G RAM/1.8TB Storage)	XXLarge	24			Month	\$1,843	65%	\$1,117
Exadata	Shared Oracle Exadata Database Computing (Licensing)	XSmall	4			Month	\$463	65%	\$281
Exadata	Shared Oracle Exadata Database Computing (Licensing)	Small	6			Month	\$695	65%	\$421
Exadata	Shared Oracle Exadata Database Computing (Licensing)	Medium	8			Month	\$927	65%	\$562
Exadata	Shared Oracle Exadata Database Computing (Licensing)	Large	12			Month	\$1,390	65%	\$843
Exadata	Shared Oracle Exadata Database Computing (Licensing)	XLarge	16			Month	\$1,854	65%	\$1,123
Exadata	Shared Oracle Exadata Database Computing (Licensing)	XXLarge	24			Month	\$2,780	65%	\$1,685

## Storage

Operating System/Platform	Storage Class	Minimum Allocation (GB)	Maximum Allocation (GB)	Unit of Service	Government List Price per GB (\$)	Percent Discount	Price per Unit of Service per GB (\$)
Oracle Linux x86-64	SAN Storage	100	Any	Month	\$0.31	65%	\$0.19
Windows 2012 Datacenter	SAN Storage	100	Any	Month	\$0.31	65%	\$0.19
Exadata	Database Storage	100	Any	Month	\$4.13	65%	\$2.50
Any	Backup	100	Any	Month	\$0.97	65%	\$0.59

Network

Service	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)	
Data Center Bandwidth (Internet)	1Mbps	\$59	65%	\$36	Monthly
MPLS Connectivity to CherryRoad Data Center	1Mbps			Provided upon request	Monthly
Managed Customer Site Router	1 router	\$165	65%	\$100	Monthly

## Disaster Recovery

Platform	Service	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)	Notes
IAAS	Setup Replication	One time cost per system	\$413	65%	\$250	5 system minimum
PAAS	Setup Replication	One time cost per database	\$2,475	65%	\$1,500	
IAAS	Disaster Declaration	One time cost per system	\$248	65%	\$150	
PAAS	Disaster Declaration	One time cost per database	\$495	65%	\$300	
IAAS	System Replication	Per system	\$50	65%	\$30	Does not include bandwidth or replicated IAAS cost
PAAS	Database Replication	Per database	\$248	65%	\$150	Does not include bandwidth or replicated IAAS cost

### *8.21 (E) Related Value-Added Services to Cloud Solutions*

Component	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)	Notes
SecureAuth - one time setup fee	\$6,600	65%	\$4,000	Minimum \$4k base pending actual scope and client requirements.
SecureAuth - ongoing user/month	\$5	65%	\$3	Per user per month - up to 500 users per client. Larger user counts will be quoted separately.

Rate Card

Position	On-Site*			Off-Site		
	Government List Price (\$)	Percent Discount	Hourly Rate (\$)	Government List Price (\$)	Percent Discount	Hourly Rate (\$)
Program Manager	\$371	65%	\$225	\$322	65%	\$195
Project Manager	\$330	65%	\$200	\$281	65%	\$170
Functional Lead	\$305	65%	\$185	\$256	65%	\$155
Specialty Products Lead	\$330	65%	\$200	\$281	65%	\$170
Technical Lead	\$305	65%	\$185	\$256	65%	\$155
Technical Developer	\$239	65%	\$145	\$182	65%	\$110
Database Administrator	\$272	65%	\$165	\$223	65%	\$135
System Administrator	\$272	65%	\$165	\$223	65%	\$135
Upgrade Specialist	\$305	65%	\$185	\$256	65%	\$155
Change Management Lead	\$272	65%	\$165	\$223	65%	\$135
Training Manager	\$305	65%	\$185	\$256	65%	\$155
Trainer	\$272	65%	\$165	\$223	65%	\$135
Security/Portal Lead	\$305	65%	\$185	\$256	65%	\$155

\* On-site rate includes all travel and expenses.



## IAAS

Operating System	Description	Memory Class	Memory Qty (# GB)	CPU Core Class	CPU Core Qty (#)	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)
Linux	Oracle Linux on Intel (64-bit)			Small	2	Month	\$97	65%	\$59
Linux	Oracle Linux on Intel (64-bit)			Medium	4	Month	\$162	65%	\$98
Linux	Oracle Linux on Intel (64-bit)			Large	8	Month	\$290	65%	\$176
Linux	Oracle Linux on Intel (64-bit)			XLarge	12	Month	\$256	65%	\$155
Linux	Oracle Linux on Intel (64-bit)			XXLarge	16	Month	\$549	65%	\$333
Linux	Additional Core			Additional	1	Month	\$54	65%	\$33
Windows	Windows 2012 Datacenter (64-bit)			Small	2	Month	\$135	65%	\$82
Windows	Windows 2012 Datacenter (64-bit)			Medium	4	Month	\$236	65%	\$143
Windows	Windows 2012 Datacenter (64-bit)			Large	8	Month	\$439	65%	\$266
Windows	Windows 2012 Datacenter (64-bit)			XLarge	12	Month	\$648	65%	\$393
Windows	Windows 2012 Datacenter (64-bit)			XXLarge	16	Month	\$853	65%	\$517
Windows	Additional Core			Additional	1	Month	\$73	65%	\$45
Linux	Oracle Linux on Intel (64-bit)	Small	4			Month	\$31	65%	\$19
Linux	Oracle Linux on Intel (64-bit)	Medium	8			Month	\$59	65%	\$36
Linux	Oracle Linux on Intel (64-bit)	Large	12			Month	\$86	65%	\$52
Linux	Oracle Linux on Intel (64-bit)	XLarge	16			Month	\$112	65%	\$68
Linux	Oracle Linux on Intel (64-bit)	XXLarge	24			Month	\$167	65%	\$101
Linux	Additional RAM	Additional	1			Month	\$8	65%	\$5
Windows	Windows 2012 Datacenter (64-bit)	Small	4			Month	\$31	65%	\$19
Windows	Windows 2012 Datacenter (64-bit)	Medium	8			Month	\$59	65%	\$36
Windows	Windows 2012 Datacenter (64-bit)	Large	12			Month	\$86	65%	\$52
Windows	Windows 2012 Datacenter (64-bit)	XLarge	16			Month	\$112	65%	\$68
Windows	Windows 2012 Datacenter (64-bit)	XXLarge	24			Month	\$167	65%	\$101
Windows	Additional RAM	Additional	1			Month	\$8	65%	\$5

PAAS

Platform	Description	Memory Class	Memory Qty (# GB)	CPU Core Class	CPU Core Qty (#)	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 16G RAM/1TB Storage)			XSmall	1	Month	\$3,446	65%	\$2,089
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only -32G RAM/2TB Storage)			Small	4	Month	\$13,786	65%	\$8,355
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only -48G RAM/3TB Storage)			Medium	8	Month	\$27,572	65%	\$16,710
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 64G RAM/4TB Storage)			Large	12	Month	\$41,357	65%	\$25,065
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 96G RAM/5TB Storage)			XLarge	24	Month	\$82,715	65%	\$50,130
Exadata	Dedicated Oracle Exadata Database Computing (Hardware only - 128G RAM/6TB Storage)			XXLarge	32	Month	\$110,286	65%	\$66,840
Exadata	Additional Dedicated Exadata Core (Hardware only - 16GB RAM/1TB Storage)			Additional	1	Month	\$4,125	65%	\$2,500
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			XSmall	1	Month	\$3,446	65%	\$2,089
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			Small	4	Month	\$13,786	65%	\$8,355
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			Medium	8	Month	\$27,572	65%	\$16,710
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			Large	12	Month	\$41,357	65%	\$25,065
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			XLarge	24	Month	\$82,715	65%	\$50,130
Exadata	Dedicated Oracle Exadata Database Computing (Licensing)			XXLarge	32	Month	\$110,286	65%	\$66,840
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 4G RAM/300GB Storage)	XSmall	4			Month	\$307	65%	\$186
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 6G RAM/450GB Storage)	Small	6			Month	\$461	65%	\$279
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 8G RAM/600GB Storage)	Medium	8			Month	\$614	65%	\$372
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 12G RAM/900GB Storage)	Large	12			Month	\$922	65%	\$559
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 24G RAM/1.2TB Storage)	XLarge	16			Month	\$1,229	65%	\$745
Exadata	Shared Oracle Exadata Database Computing (Hardware only - 32G RAM/1.8TB Storage)	XXLarge	24			Month	\$1,843	65%	\$1,117
Exadata	Shared Oracle Exadata Database Computing (Licensing)	XSmall	4			Month	\$463	65%	\$281
Exadata	Shared Oracle Exadata Database Computing (Licensing)	Small	6			Month	\$695	65%	\$421
Exadata	Shared Oracle Exadata Database Computing (Licensing)	Medium	8			Month	\$927	65%	\$562
Exadata	Shared Oracle Exadata Database Computing (Licensing)	Large	12			Month	\$1,390	65%	\$843
Exadata	Shared Oracle Exadata Database Computing (Licensing)	XLarge	16			Month	\$1,854	65%	\$1,123
Exadata	Shared Oracle Exadata Database Computing (Licensing)	XXLarge	24			Month	\$2,780	65%	\$1,685

Storage

Operating System/Platform	Storage Class	Minimum Allocation (GB)	Maximum Allocation (GB)	Unit of Service	Government List Price per GB (\$)	Percent Discount	Price per Unit of Service per GB (\$)
Oracle Linux x86-64	SAN Storage	100	Any	Month	\$0.31	65%	\$0.19
Windows 2012 Datacenter	SAN Storage	100	Any	Month	\$0.31	65%	\$0.19
Exadata	Database Storage	100	Any	Month	\$4.13	65%	\$2.50
Any	Backup	100	Any	Month	\$0.97	65%	\$0.59

Network

Service	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)	
Data Center Bandwidth (Internet)	1Mbps	\$59	65%	\$36	Monthly
MPLS Connectivity to CherryRoad Data Center	1Mbps			Provided upon request	Monthly
Managed Customer Site Router	1 router	\$165	65%	\$100	Monthly

Disaster Recovery

Platform	Service	Unit of Service	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)	Notes
IAAS	Setup Replication	One time cost per system	\$413	65%	\$250	5 system minimum
PAAS	Setup Replication	One time cost per database	\$2,475	65%	\$1,500	
IAAS	Disaster Declaration	One time cost per system	\$248	65%	\$150	
PAAS	Disaster Declaration	One time cost per database	\$495	65%	\$300	
IAAS	System Replication	Per system	\$50	65%	\$30	Does not include bandwidth or replicated IAAS cost
PAAS	Database Replication	Per database	\$248	65%	\$150	Does not include bandwidth or replicated IAAS cost

***8.21 (E) Related Value-Added Services to Cloud Solutions***

Component	Government List Price (\$)	Percent Discount	Cost Per Unit of Service (\$)	Notes
SecureAuth - one time setup fee	\$6,600	65%	\$4,000	Minimum \$4k base pending actual scope and client requirements.
SecureAuth - ongoing user/month	\$5	65%	\$3	Per user per month - up to 500 users per client. Larger user counts will be quoted separately.

Rate Card

Position	On-Site*			Off-Site		
	Government List Price (\$)	Percent Discount	Hourly Rate (\$)	Government List Price (\$)	Percent Discount	Hourly Rate (\$)
Program Manager	\$371	65%	\$225	\$322	65%	\$195
Project Manager	\$330	65%	\$200	\$281	65%	\$170
Functional Lead	\$305	65%	\$185	\$256	65%	\$155
Specialty Products Lead	\$330	65%	\$200	\$281	65%	\$170
Technical Lead	\$305	65%	\$185	\$256	65%	\$155
Technical Developer	\$239	65%	\$145	\$182	65%	\$110
Database Administrator	\$272	65%	\$165	\$223	65%	\$135
System Administrator	\$272	65%	\$165	\$223	65%	\$135
Upgrade Specialist	\$305	65%	\$185	\$256	65%	\$155
Change Management Lead	\$272	65%	\$165	\$223	65%	\$135
Training Manager	\$305	65%	\$185	\$256	65%	\$155
Trainer	\$272	65%	\$165	\$223	65%	\$135
Security/Portal Lead	\$305	65%	\$185	\$256	65%	\$155

\* On-site rate includes all travel and expenses.



**Proposal for an NASPO ValuePoint Cloud Solutions for the  
State of Utah**

**Solicitation CH16012**

March 10, 2016

**TECHNICAL PROPOSAL**





## *5.2 Cover Letter*

Please see CherryRoad's signed cover letter:

- **Cover Letter – CherryRoad.pdf**









# Table of Contents

<b>1. RFP Signature Page.....</b>	<b>1</b>
<b>2. Executive Summary.....</b>	<b>2</b>
CherryRoad Company Overview .....	2
CherryRoad IaaS and PaaS Service Offerings .....	2
<b>3. Mandatory Minimums .....</b>	<b>5</b>
5.2 Cover Letter .....	5
5.3 Acknowledgement of Amendments .....	5
5.5 General Requirements for the Service Offerings .....	5
5.7 Recertification of Mandatory Minimums and Technical Specifications .....	7
<b>4. Business Profile.....</b>	<b>8</b>
6.1 (M) (E) Business Profile .....	8
6.2 (M) (E) Scope of Experience.....	9
6.3 (M) Financials .....	14
6.4 (E) General Information .....	15
6.5 (E) Billing and Pricing Practices .....	16
6.6 (E) Scope and Variety of Cloud Solutions.....	17
6.7 (E) Best Practices .....	19
<b>5. Organization Profile.....</b>	<b>21</b>
7.1 (ME) Contract Manager .....	21
<b>6. Technical Response .....</b>	<b>30</b>
8.1 (M) (E) Technical Requirements .....	32
8.2 (E) Subcontractors .....	36
8.3 (E) Working with Purchasing Entities .....	37
8.4 (E) Customer Service.....	40
8.5 (E) Security of Information .....	42
8.6 (E) Privacy and Security .....	43
8.7 (E) Migration and Redeployment Plan .....	49
8.8 (E) Service or Data Recovery .....	50
8.9 (E) Data Protection .....	51
8.10 (E) Service Level Agreements .....	52
8.11 (E) Data Disposal.....	54
8.12 (E) Performance Measures and Reporting .....	55
8.13 (E) Cloud Security Alliance Questionnaires .....	58
8.14 (E) Service Provisioning.....	59
8.15 (E) Back Up And Disaster Plan.....	60
8.16 (E) Solution Administration .....	61
8.17 (E) Hosting and Provisioning .....	62
8.18 (E) Trial and Testing Periods (Pre- and Post-Purchase) .....	64
8.19 (E) Integration and Customization .....	65
8.20 (E) Marketing Plan .....	66
8.21 (E) Related Value-Added Services to Cloud Solutions .....	67
8.22 (E) Supporting Infrastructure.....	68
8.23 (E) Alignment of Cloud Computing Reference Architecture.....	69
<b>7. Confidential, Protected or Proprietary Information .....</b>	<b>70</b>
<b>8. Exceptions and/or Additions to the Standard Terms and Conditions .....</b>	<b>72</b>



The State of Utah.....72

**9. Cost Proposal .....75**

**Acknowledgement of Amendments .....76**

**Vendor Information Form.....77**



## 1. RFP Signature Page

*The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of the RFP.*

*Proposals must be submitted with a state supplied signature page, located on Bidsync as an attachment to the RFP, which must contain an ORIGINAL HANDWRITTEN signature executed in INK OR AN ELECTRONIC SIGNATURE, and be returned with the relevant Solicitation documents. PHOTOCOPIED SIGNATURES or FACSIMILE SIGNATURES are NOT ACCEPTABLE (and will result in a finding that your proposal is non-responsive). The Signature Page should be named "Signature Page" is submitted electronically and if submitted manually then it should be the first page included in your proposal packet. The Signature Page includes General Provisions, which are relevant to the RFP.*

CherryRoad has attached its signed Proposal Signature page and Vendor Information Form.

Please see:

- **Signature Page – CherryRoad.pdf**













## 2. Executive Summary

*The one or two page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The Lead State should be able to determine the essence of the Proposal by reading the executive summary. See Section 5.4 of the RFP.*

*Offerors must provide an Executive Summary of its proposal. An Executive Summary should highlight the major features of an Offeror's proposal. Briefly describe the proposal in no more than three (3) pages. The evaluation committee should be able to determine the essence of the proposal by reading the Executive Summary. Any requirements that cannot be met by the Offeror must be included.*

The State of Utah is seeking to establish a Master Agreement with qualified vendors to provide services related to cloud solutions for all participating entities through NASPO ValuePoint Cooperative Purchasing Program. The goal of the RFP is to provide the best value, and achieve more favorable pricing through the collective volume of potential purchases by numerous state and local government entities. The Agreements will supply high-quality, cloud-based service providers that have the ability to provide a menu of cloud solution offerings that will increase the technology department's overall efficiencies, reduce costs, improve operational scalability, provide business continuity, increase collaboration efficiencies, and allow for expanded flexibility in work practices and system improvements.

The awarded contracts will allow the participating entities access to technical capabilities that run in cloud environments and meet NIST Essential Characteristics. Categories in scope include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

### *CherryRoad Company Overview*

CherryRoad is a full-service system integrator with a focus on supporting clients in the public sector in various Oracle technology initiatives. As an Oracle Platinum partner, we provide private cloud services (IaaS and PaaS), ERP systems implementations and upgrades, custom development, and support services that help maximize Oracle's systems' performance. We have been providing technology solutions to state and local governments for over 20 years and have developed the products and tools needed to support the cloud technology initiatives outlined in this RFP.

### *CherryRoad IaaS and PaaS Service Offerings*

CherryRoad's cloud solutions (IaaS and PaaS) were developed specifically for state and local government. We leveraged our platform and infrastructure experience attained by working with 14 states including the States of Oklahoma, Vermont, New Mexico, Tennessee, and Delaware. While working with hundreds of state agencies, CherryRoad learned that three components for state infrastructure and platform requirements stood out: **Security**, **Performance**, and a **Voice**. The requirements and liability of **Securing** personal, identifiable information has never been more important. The need for processing massing data transactions at the state level requires the highest **Performing** technology. And finally, ever-changing regulatory and compliance updates drive the need for states to have a **Voice** regarding their cloud requirements. CherryRoad saw that large public cloud providers could not provide solutions to government with these attributes. That's why CherryRoad built our IaaS and PaaS solutions specifically for state and local government. Our infrastructure, security,



processes, and controls are designed to meet government compliance requirements and allow clients to have a voice regarding what advancements and updates should be made in the future. Our solutions are designed from top to bottom for government, no labor or data information crosses U.S. borders, and all storage, monitoring, and access of data is confined within the U.S.

### Infrastructure as a Service (IaaS)

CherryRoad's Infrastructure as a Service (IaaS) offers a set of core infrastructure capabilities such as elastic compute and storage to provide our clients the ability to run any workload in our cloud. Specifically for developers, infrastructure services will include:

- *Compute Service* to leverage elastic compute capacity to address growing business needs.
- *Storage Service* to provide a secure, scalable, reliable, and simple storage solution to meet all of your enterprise needs.
- *Messaging Service* to leverage dynamic messaging capabilities for workflow agility.

### Platform as a Service (PaaS)

CherryRoad's PaaS solutions offer our clients the necessary tools help your organization innovate faster, increase productivity, and reduce costs. Our offerings include:

- **Application Development** – In order to help our clients reduce the cost of developing, testing, and deploying applications CherryRoad utilizes our platform to roll out critical application development services. These service offerings allow our clients to develop and deploy nearly any type of application, including enterprise apps, lightweight container apps, web apps, mobile apps, and more. We utilize Oracle products that are based on prevailing Java standards, so development teams can use familiar architectures, utilities, and products.
- **Data Management** – Utilizing our Exadata systems, our clients can easily embark on a pure CherryRoad cloud or hybrid cloud strategy that spans on-premises databases as well as databases in the cloud. Our Exadata services offer immediate business benefits to a broad range of customers including the following benefits:
  - Existing Oracle Database customers who are not on Exadata can start getting the benefits of increased performance, availability, and scalability benefits without losing any of the database functionality they rely on.
  - Organizations that are utilizing other public cloud databases with limited functionality and compromised data consistency can move to the most sophisticated database functionality on the most powerful private cloud database platform.
- **Business Analytics** – Utilizing our platform, we can deliver Oracle's Business Analytics which provides an unmatched user experience with the ease and flexibility you need from your analytics system. Combine any data from any source for a complete view of your business.
- **Integration** – Integration Services simplify and accelerate integration of our cloud and your on-premises applications. With comprehensive cloud-based integration, you can maximize the value of data and create innovative services with greater agility and reduced risk.



- **Content and Process** – Organizations need cloud-based services that can blend content, people, processes, and communications as part of a cohesive workflow. The State can utilize a new generation of connected tools that drive meaningful collaboration and mobility.



## 3. Mandatory Minimums

*This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.*

### 5.2 Cover Letter

Please find CherryRoad's cover letter at the very beginning of this response, after the cover page.

### 5.3 Acknowledgement of Amendments

Please find CherryRoad's signed acknowledgements in the last section of this response.

### 5.5 General Requirements for the Service Offerings

*5.5.1 Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.*

CherryRoad agrees to provide a usage report administrator responsible for the quarterly sales reporting described in the in the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

*5.5.2 Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.*

CherryRoad agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

*5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment . Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), **Exhibit 1 to Attachment B**, or submit a report documenting compliance with Cloud Controls Matrix (CCM), **Exhibit 2 to Attachment B**. Offeror must also represent and warrant the accuracy and currency of the information on the completed. **Offerors are encouraged to complete and submit both exhibits to Attachment B.***

CherryRoad has completed CSA STAR Registry Self-Assessment and has submitted the Consensus Assessments Initiative Questionnaire (CAIQ), **Exhibit 1 to Attachment B**

Please see:

- **Technical Response – 8.13 b – CherryRoad Exhibit 1.xlsx**



*5.5.4 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.*

CherryRoad has provided a sample of its Service Level Agreements (SLA). The Sample SLA can be found in section 8.10 of this response.





## *5.7 Recertification of Mandatory Minimums and Technical Specifications*

*Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.*

CherryRoad acknowledges that if awarded a contract under the RFP that it will annually certify to the lead state that it still meets or exceeds the technical capabilities discussed in this proposal.



## 4. Business Profile

*This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.*

### 6. Business Information

#### 6.1 (M) (E) Business Profile

*Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. **Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award.***

CherryRoad Technologies Inc. provides Cloud Services, systems implementations, integrations, upgrades, and consulting services that maximize ERP system performance for the public sectors. For three decades, CherryRoad has earned a solid reputation for combining our technological, organizational, functional, and vertical market expertise into practical solutions that deliver results, specifically with Oracle's applications. Our flexible approach and methodologies enable us to structure engagements that best meet our clients' specific needs.

Key Services	
<b>Enterprise Solutions</b>	Strategy assessments, enterprise application integration, software implementations, upgrades, training, and production support for Oracle Enterprise Resource Planning (ERP) PeopleSoft, E-Business, and Cloud suites.
<b>Oracle Fusion Implementation Services</b>	Dedicated certified team to provide best practice implementations and guidance for net new adoption, co-existence, or migration from existing systems.
<b>Cloud Services IaaS PaaS</b>	Application hosting services for the entire technology stack including physical infrastructure, security network, communications infrastructure, hardware, operating systems, database, and disaster recovery in our world-class data centers.
<b>Application Support Services</b>	Oracle application on-site and remote functional and technical support services backed by 24x7 help desk support.
<b>Management Consulting</b>	Strategy/Visioning, Change Management, Software Selection, and Business Process Optimization services.
<b>Enterprise Architecture</b>	Current and future state architecture definitions, future state roadmap development, and overall information technology (IT) and IT strategy assessment services.
<b>Business Intelligence</b>	Proactive intelligence, real-time predictive analytics, and scalable solutions that are enterprise-wide or local to one division, department, or project.



## Office Locations

Headquartered in Morris Plains, NJ, CherryRoad has additional offices in Boca Raton, FL; Chicago, IL; and Sacramento, CA. We employ 175 full-time consultants who manage concurrent projects nationwide.

## Steady Growth

CherryRoad's financial strength is demonstrated by our consistent stability and growth. In 2015, we acquired the Oracle practice, including the E-Business and Cloud activities, of Strategic Information Solutions, Inc. (SIS). This purchase was preceded by our acquisition in 2009 of the Oracle PeopleSoft practice of Towers Watson, a global provider of HR consultancy services, and our 2010 acquisition of the Maximus ERP Solutions Division, a top provider of PeopleSoft implementation services at the state level.

CherryRoad has a stable management team charting its course. The firm's founders and original executive management team are actively involved in the day-to-day management of the business.

## Best Diversity Company Award Winner

CherryRoad was recently voted by the readers of *Diversity/Careers in Engineering & Information Technology Magazine* as a 2014 "Best Diversity Company" in recognition of our support of minorities, women, veterans, attention to work/life balance, and commitment to diversity.



## **6.2 (M) (E) Scope of Experience**

*Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided Solutions identical or very similar to those required by this RFP. Government experience is preferred.*

CherryRoad is a leading Oracle partner specializing in cloud, implementation, upgrade, and support services for Oracle clients within the public sector. The CherryRoad team brings to the State an unparalleled track record of experience and success in providing total business results to government agencies across the country.

Similar Public Sector cloud-based hosting projects include:

### San Diego Office of Education

**Cloud Contract value 1.2 million per year on a three-year contract.**

The San Diego County Office of Education (SDCOE) includes 42 K-12 school districts, and five community colleges servicing hundreds of thousands of students. SDCOE has fiscal oversight of school districts and provides other required and optional services such as retirement reporting, credential auditing, intermediary between the State and the County of San Diego, County Treasury,



commercial warrant auditing, and other various support functions. The County processes almost 668,000 payroll warrants per year for 72,000 employees. On average, 55,000 people are paid each month. It also processes more than 135,000 commercial warrants annually for the local school districts.



CherryRoad was chosen to implement, **host**, and support SDCOE's PeopleSoft Financials and HCM version 9.2, as well as ECM, Hyperion, and Oracle Business Intelligence. The objectives of the project include modernizing and improving systems while reducing the long-term total cost of ownership. The solution will integrate critical business processes including payroll, human resources, financial accounting, and business operations across the organizations. It will also modernize recording, tracking, and managing of internal and external human resources activities, including standardization across districts, while recognizing district-specific needs and automation of manual processes

As part of PeopleSoft FIN, HCM, and Portal implementation project, CherryRoad provides Oracle Database support and management services including:

- **Installation and configuration of Oracle Real Application Clusters and Oracle RDBMS 11.2.0 on Linux RedHat platform**
- **Installation of Oracle RDBMS on Oracle Engineered Exadata platform**
- **Simultaneous management of 150+ databases**
- Oracle database configuration for PeopleSoft environments
- **Installation and configuration of Oracle Enterprise Manager Grid Control 11g in order to monitor, manage, and tune Oracle databases**
- Implementation of disaster recovery plan based on Oracle Dataguard technology
- **Several production databases running in NJ data center are being continuously replicated to Dataguard standby databases in CA data center**
- **Database availability monitoring and notifications**
- Database performance monitoring and SQL tuning
- Implementation of RMAN hot and cold backup and recovery process
- Implementation of scripted and scheduled automatic and ad hoc process of Development database refresh from copy of production

### Orange County, NY

**Cloud contract value: \$250,000 per year on a three-year contract.**



Orange County is part of the Poughkeepsie-Newburgh-Middletown, NY Metropolitan area. It is in the state's scenic Mid-Hudson region of the Hudson Valley

CherryRoad was selected to provide **Hosting** and Help Desk services to support the Oracle E-Business suite of applications and infrastructure. The County was struggling to support their enterprise systems with a combination of in-house staff and outside contractors.

**CherryRoad provides Hosting and Disaster Recovery support for hardware, operating systems, operational services, database administration services, systems administration services, and application management services.**



As part of ongoing support, CherryRoad works with the County to provide continuous improvement, helping to maximize the ROI on their ERP system.

Support benefits include:

- Reduction in County's current service response time
- Reduced capital expenditures
- Flexibility to scale infrastructure up or down on-demand
- Extend Oracle support staff skills through vendor's resources
- Improved service levels
- More efficient utilization of County functional staff
- Safe, secure, and auditable data center infrastructure
- Secure backup services with recoverable data

In addition, CherryRoad recently conducted a database upgrade from RDBMS 10.2.0.4 to RDBMS 11.2.0.4 (i.e. 11gR2).

### Georgia State Financing and Investment commission

**Cloud contract value: \$120,000 per year on a three-year contract.**



The Georgia State Financing and Investment Commission (GSFIC) manages the proper application of proceeds from general obligation debt and the issuance of all public debt by the State.

GSFIC is responsible for the planning, scheduling, selling, and delivery of general obligation bonds, including the investment and accounting of all proceeds from the issuance of these bonds or from other amounts appropriated by the Legislature for capital outlay purposes.

As partners for 17+ years, CherryRoad and GSFIC completed many successful projects ranging from the initial implementation to the most recent PeopleSoft Financials upgrade to version 9.2 and PeopleTools 8.54, with the Microsoft SQL Server database upgrade to 2012.

After the implementation of PeopleSoft version 7.0, GSFIC struggled with the software and hardware demands required to support and maintain the system and turned to CherryRoad for a solution.

In 1999, CherryRoad began the process of 'Upgrade to Hosting' the application. **In 2000, the application was live on the CherryRoad Public Sector Cloud. This Cloud migration included a database conversion from the Oracle platform to MicroSoft SQL Server and an application upgrade to the latest PeopleTools version 7.5.**

Today, CherryRoad continues to provide 24x7 support, including technical and functional support utilizing our Managed Services Help Desk. These support services include on-demand PeopleSoft customizations, expert support with functional processing and/or configuration challenges, as well as performance tuning and regular and standard hardware and software maintenance.

CherryRoad and GSFIC have shared many accomplishments while keeping the PeopleSoft application certified and compliant, including four full PeopleSoft application upgrades. During these, CherryRoad



managed the processes performing all technical retrofits and new development as well as complete functional regression testing on the new systems.

### University of Texas – Dallas

**Cloud contract value: \$960,000 per year on a two-year contract.**

Opened in 1969, UT Dallas has evolved into one of the best research institutions in Texas. With 133-degree programs, the university attracts the brightest minds in science, math, and engineering and boasts one of the top business schools in the state. An ever-expanding breadth of degree programs and capital improvements to the campus promise to push UT Dallas to the forefront of education excellence.



UT Dallas has approximately 23,000 students and 79,938 alumni.

**CherryRoad was selected to provide hosted and managed services to include disaster recovery (DR) for all Oracle and PeopleSoft integrated environments (production and non-production) for currently implemented UTD ERP systems which include HCM, Financials, Campus Solutions, OBIEE, and STAT environments.**

CherryRoad created a DR solution for the University that utilizes Oracle Exadata for real time DB replication. A hot site where live VMs are running is maintained with nightly refreshes of data. Data backup and restore are handled by Commvault Simpana and stored on tape and EMC DataDomain.

### Miami Children's Health System

**Cloud contract value: \$240,000 for a three-year contract.**



**Miami Children's Health System** is South Florida's only licensed specialty hospital exclusively for children with more than 650 attending physicians and over 130 pediatric sub-specialists. The 289-bed hospital is renowned for excellence in all aspects of pediatric medicine and is routinely ranked among the best children's hospitals in the nation. MCH is one of the largest employers in Miami-Dade County in 2014 with over 3,500 employees.

MCH is implementing PeopleSoft 9.2 Financials, HCM, and Supply Chain Management applications. **CherryRoad is providing IaaS and PaaS for the entire technology stack including physical infrastructure, security, network, communications infrastructure, hardware, operating system, and database in our facilities. Each of the following services are being provided for all Non-Production and Production environments.**



- **Operating System Management** – Manage operating system security, and monitor performance.
- **Infrastructure Patches and Fixes** –, apply standard infrastructure patches
- **Hosting Facility (Data Center)** – Maintain physical security of the hosting facility and maintain inventory of assets.
- **Storage Management** – Monitor/maintain file systems, provide offsite storage, and monitor/maintain storage for database instances.
- **Network Management** – Maintain and monitor all network LANs and VLANs within the hosting



facility. **Backup/Restore/Disaster Recovery Management** – Setup and configure backups and monitoring and recover the environment in the event of a disaster.

- **Monitoring, Event Detection, and Notification** – Identify initial hardware, OS, LAN, database, and software monitoring requirements, **Database Administration** – Administer database instances including configuration, sizing, ongoing storage management,.
- **Oracle Software Architecture Administration** – Configure and maintain server environments and provide routine reboots of server components according to schedule.
- **Help Desk/Client Management/Project Management** – Address issues and problems arising from the services
- **Application Patching** – Provide technical support to apply application patching two times per year. Tax updates and regulatory patching applied when released.
- **Oracle Application Performance and Tuning** – Monitor application availability, identify software or service issues. Facilitate the analysis of performance bottlenecks and assist in troubleshooting application performance issues.





## 6.3 (M) Financials

*Offeror must provide audited financial statements to the State and should meet a minimum Dun and Bradstreet (D&B) credit rating of 4A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.*

CherryRoad has provided the following information in separate documents:

- **Business Profile – 6.3 Financials – CherryRoad Dun and Bradstreet Report.pdf**
- **Business Profile – 6.3 Financials – CherryRoad Confidential Audited Financial Statement 2014-2015.pdf**
- **Business Profile – 6.3 Financials – CherryRoad Letter to Accompany Audited Financial Statement.pdf**





## 6.4 (E) General Information

*6.4.1 Provide any pertinent general information about the depth and breadth of your services and their overall use and acceptance in the cloud marketplace.*

The focus of CherryRoad's response is to provide Infrastructure- and Platform as a Service (IaaS and PaaS) services to the State. Building on our ERP consulting and hosting experience, CherryRoad has developed a total Managed Services solution for state and local government market that brings IaaS, PaaS, support, and continuous improvement to our clients.

Our Managed Service solution, used in part by organizations such as the states of Georgia, Indiana, Minnesota, Delaware, and the San Diego Office of Education, will provide the State a one-stop solution, built on Oracle Engineered Systems and housed in CherryRoad's Tier 3 data centers. CherryRoad's support solution has been built from the ground up specifically public sector. Our infrastructure, security, processes, and controls were all designed to meet state and local government compliance requirements. CherryRoad takes industry standard current and future security and compliance requirements very seriously, and that is why our solution does not allow any labor or data to cross U.S. borders. This includes the storage, monitoring, and accessing of data. Mission critical systems will be maintained, users will be supported, and continuous process improvement will be delivered. The benefit to our clients is this allows them to focus on core constituent service objectives while CherryRoad handles the day-to-day maintenance and upkeep of the system.

Oracle Engineered Systems combine best-of-breed hardware and software components and achieves the goals of improving computing performance by preconfiguring each of the technology layers to work together in an optimal fashion. Designed, engineered, and tested to work best together, Oracle Engineered Systems are optimized for world class performance. The CherryRoad solution is cutting edge within the public sector and offers our clients speed and efficient systems at a fraction of the cost. While it is important for our clients to understand the infrastructure and technology that will support your applications, it is even more meaningful to understand the benefits of that technology to your business and your users. The infrastructure solution that CherryRoad is proposing utilizes Oracle's Exadata and places our clients in the best position to:

- Attain the maximum service level agreements for performance. Solutions based from a commodity technology build out will not attain the performance levels of our solution.
- Reduce points of failure. Engineered Systems are designed to be fully integrated and remove single points of failure. This translates to maximum availability and reduced risk to our clients.

*6.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.*

Utilizing our existing architecture and datacenters, our CherryRoad Managed Services team can create test or proof of concept environments to allow an entity to verify we have met mandatory requirements at multiple levels. Whether it involves utilizing our Help Desk, creating an instance for use, and/or making a tool available CherryRoad's team will work with the specific entity as needed.



## 6.5 (E) Billing and Pricing Practices

*DO NOT INCLUDE YOUR PRICING CATALOG, as part of your response to this question.*

*6.5.1 Specify your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.*

CherryRoad offers flexible billing practices to meet our client's needs. Our typical cloud-based services pricing structure is an all-inclusive, fixed monthly fee for a term of 3-5 years. Additional fixed priced project work can be billed on an agreed upon deliverables based schedule. We also have enclosed our rate card in the pricing section of the proposal for any Time and Material work.

*6.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.*

There is typically a transition fee when moving from an on premise or existing system to a cloud based platform. This is usually a fixed cost fee and can be paid semi-monthly or incorporated into the long-term fixed monthly services fee.

*6.5.3 Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.*

CherryRoad Cloud systems are designed on the NIST cloud architecture model. Tools used to monitor and report on usage and billing information have been described earlier in this response.



## 6.6 (E) Scope and Variety of Cloud Solutions

*Specify the scope and variety of the service models you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer.*

The focus of CherryRoad's response is around IaaS and PaaS services utilizing our Exa engineered systems platform within our state of the art hosting facilities. Our services include but are not limited to:

### Infrastructure as a Service (IaaS)

CherryRoad's Infrastructure as a Service (IaaS) offers a set of core infrastructure capabilities like elastic compute and storage to provide our clients the ability to run any workload in our cloud. Specifically for developers, infrastructure services will include:

- *Compute Service* to leverage elastic compute capacity to address growing business needs.
- *Storage Service* to provide a secure, scalable, reliable, and simple storage solution to meet all of your enterprise needs.
- *Messaging Service* to leverage dynamic messaging capabilities for workflow agility.

### Platform as a Service (PaaS)

CherryRoad's PaaS solutions offers our clients the necessary tools help your organization innovate faster, increase productivity, and reduce costs. Our offerings include:

- *Application development* - In order to help our clients reduce the cost of developing, testing, and deploying applications CherryRoad utilizes our platform to roll out critical application development services. These services offerings allow our clients to develop and deploy nearly any type of application, including enterprise apps, lightweight container apps, web apps, mobile apps, and more. We utilize Oracle products that are based on prevailing Java standards, so development teams can use familiar architectures, utilities, and products.
- *Data Management* – Utilizing our Exadata systems our clients can easily embark on a pure CherryRoad cloud or hybrid cloud strategy that spans on-premises databases as well as databases in the Cloud. Our Exadata Services offer immediate business benefits to a broad range of customers including the following benefits:
  - Existing Oracle Database customers who are not on Exadata can start getting the benefits of increased performance, availability and scalability benefits without losing any of the database functionality they rely on.
  - Organizations that are utilizing other public cloud databases with limited functionality and compromised data consistency can move to the most sophisticated database functionality on the most powerful private cloud database platform.
- *Business Analytics* – Utilizing our platform we can deliver Oracle's Business Analytics which provides unmatched user experience with the ease and flexibility you need from your analytics system. Combine any data from any source for a complete view of your business.



- *Integration* – Integration Services simplify and accelerate integration of our cloud and your on-premises applications. With comprehensive cloud-based integration, you can maximize the value of data and create innovative services with greater agility and reduced risk.
- *Content and Process* – Organizations need cloud-based services that can blend content, people, processes, and communications as part of a cohesive workflow. The State can utilize a new generation of connected tools that drive meaningful collaboration and mobility.



## 6.7 (E) Best Practices

*Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.*

CherryRoad is committed to providing safe and secure systems using industry best practices. Our policy and practice of constant improvement is designed to ensure that industry best practices are implemented at all times.

Some of the services provided today are:

- Anti-virus is run on all systems and maintained by our operations staff.
- Host Based IDS is run on all systems and maintained by our operations staff.
- Firewalls protect the outside perimeter for both internet and private networks. They provide for segregation of data and a choke point for unauthorized data access. The CherryRoad network team supports these devices and all security data is reviewed to detect any unwanted activity.
- Network IDS is employed to not only detect but to deter unwanted activity to protect the integrity and availability of the data transporting over CherryRoad networks.
- Physical Network separation of all client data to ensure privacy and security.
- SIEM system monitoring to monitor all vital infrastructures.
- All data at rest is encrypted to ensure privacy while at rest.
- All offsite tape data is encrypted to ensure privacy from outside threats.
- All user accounts are individual and subscribe to least privilege.
- Data Center physical security requires badged user 24x7x365 guarded to thwart any unauthorized access to infrastructure or media containing client data.
- All equipment is physically secured in locked cages on datacenter floor.
- VPN encrypted access with two factor authentication.
- All supported applications, databases and network are hardened according to industry best practices and validated via annual independent audits:
  - SSAE-16
  - HIPPA
  - NIST 800-53
  - PCI
  - 27001
  - CSA

CherryRoad currently employs the following policies and standards to ensure data confidentiality.

- Access credentials utilize best practice of least privileged.
- Every administrative user must have their own named account.
- Remote Administrator Access Process: Requires two factor authentication and secure VPN with encryption.
- Password Administration policy
- PC acceptable use policy/
- User Administration policy



- Employment termination and account removal process.

CherryRoad and industry best practice require that all user access is reviewed on a regular basis. Access credentials are locked out after five unsuccessful attempts. CherryRoad administrative user account access is reviewable annually and is restricted to least privilege.



## 5. Organization Profile

*This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.*

### 7. Organization and Staffing

*This Section focuses on the individual persons and roles that will be involved in performance of the Master Agreement. The State has identified a number of roles that are necessary based on the requirements of Attachment D; these titles are not meant to be restrictive, but are used to identify key roles. The State recognizes that different Offerors may use different titles, have different organizational structures, and employ roles that have not been specifically identified by the State. For the roles that have been identified, provide the required information about the person/role that will meet the requirements identified by the State; feel free to provide the title your business uses for that role. If multiple identified roles are performed by the same person, be sure to include that information in your response.*

### 7.1 (ME) Contract Manager

*The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. **The Contract Manager must have experience managing contracts for cloud solutions.***

Our proposed Contract Manager has over five years of experience managing contracts for cloud-based solutions.

*7.1.1 Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.*

Nazgol Khamneipur PMP  
415-722-6461  
[nkhamneipur@cherryroad.com](mailto:nkhamneipur@cherryroad.com)  
Availability: 8 am to 5 pm CST

*7.1.2 **Describe in detail** the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. **Provide a detailed resume for the Contract Manager.***

Nazgol Khamneipur has over twelve years' experience managing large contracts for Public sector clients, including many States, Counties, and Cities. She currently provides contract management and reporting services for our cloud and Managed Services accounts.

**Nazgol R. Khamneipur, PMP**  
Contract Manager/Contract  
Administrator

- Certified Project Management Professional (PMP)
- PeopleSoft Certified HRMS Consultant, Financial Consultant, and Technology Consultant



	<ul style="list-style-type: none"><li>• More than 16+ years of experience with IT implementation and upgrade projects</li><li>• In-depth experience in management and supervision of developers, analysts, programmers, and leads; as well as hiring, budgeting, revenue tracking, profit and loss accountability.</li><li>• Recent projects include Kern High School District, CA; State of Minnesota; Georgia State Financing &amp; Investment Commission (GSFIC); Sonoma County, CA; and University of Texas-Dallas</li></ul>
--	--

Nazgol’s resume follows.





## NAZGOL R. KHAMNEIPUR, PMP

### Director - Support Services

#### Experience Summary

Project Manager with over sixteen years of experience in implementation projects, twelve of which are in Public Sector administration with State government and Transportation. Extensive business process and technical knowledge as well as a track record of sustaining HCM and Financial applications. Highly organized.

#### Project Summary

<b>Client Names</b>	<b>Role On Project</b>	<b>Dates On Project</b>
Atlantic Health Systems	Service Delivery Manager	03/16 – Present
City of Seattle, WA	Service Delivery Manager	02/16 – Present
City of San Jose, CA	Service Delivery Manager	02/16 – Present
Miami Children's Hospital	Service Delivery Manager	02/16 – Present
CherryRoad Managed Services	Director of Support Services	05/15 – Present
State of Minnesota	Service Delivery Manager	05/15 – Present
Georgia State Financing & Investment Commission (GSFIC)	Service Delivery Manager	05/15 – Present
Sonoma County, CA	Service Delivery Manager	03/15 – Present
Indiana Public Retirement System (INPRS)	Service Delivery Manager	05/14 – Present
CherryRoad Managed Services	PMO	01/14 – 04/15
San Diego County of Education (SDCOE), CA	Service Delivery Manager	09/13 – Present
City & County of San Francisco Controller's Office (CCSF), CA	Service Delivery Manager	09/13 – 04/15
Ramsey County, MN	Project Manager	05/13 – 07/31
State of Minnesota	Project Manager	11/11 – 04/13
Cognizant	Functional Consultant	09/11 – 11/11
State of Minnesota	Project Team Lead	02/10 – 07/11
Bay Area Rapid Transport District (BART)	Project Manager	12/04 – 02/10

#### Skills Summary

##### **Certifications & Training:**

- Certified Project Management Professional (PMP), 2011
- Sun Certified Programmer for Java 2 Platform, 2002
- Project Management for IT Professionals, International Institute of Learning, 2002
- PeopleSoft Certified HRMS, Financial Management, & Technology Consultant, 2001

##### **PeopleSoft Experience:**

- 16+ years

- Employee/Manager Self-Service
- Workforce Administration

##### **Public Sector Experience:**

- 12 years

##### **PeopleTools:**

- PeopleCode
- Workflow
- Application Engine
- Crystal/Query
- Tree Manager
- nVision
- Process Scheduler
- Security Administration

##### **PeopleSoft Modules:**

- Billing
- Accounts Receivable
- General Ledger
- Commitment Control
- Project Costing
- Human Resources
- Base Benefits, Benefits Administration
- Profile Management
- eProfile
- Position Management

##### **Methodologies:**

- MTK
- Software Development Life Cycle
- Project Management for IT Professionals



## Professional Experience Summary

**Client Name:** *Atlantic Health Systems*  
**Role(s) on Project:** *Service Delivery Manager*  
**Module(s):** *PeopleSoft HCM*  
**Environment:** *PeopleSoft v9.2*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *City of Seattle, WA*  
**Role(s) on Project:** *Service Delivery Manager*  
**Module(s):** *PeopleSoft FMS*  
**Environment:** *PeopleSoft v9.2*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *City of San Jose, CA*  
**Role(s) on Project:** *Service Delivery Manager*  
**Module(s):** *PeopleSoft HCM, Hyperion, Taleo*  
**Environment:** *PeopleSoft v9.2*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *Miami Children's Hospital*  
**Role(s) on Project:** *Service Delivery Manager*  
**Module(s):** *PeopleSoft HCM & FMS*  
**Environment:** *PeopleSoft v9.2*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *CherryRoad Managed Services*  
**Role(s) on Project:** *Director of Support Services*

- Responsible for all Managed Services Support Engagements.
- Manage all Application Support resources for Managed Services.
- Develop standardized policies and processes to be followed by the managed services team.
- Work with PM/Service Delivery Manager/Transition Manager to improve project efficiency and communication.



- Report on project metrics to CherryRoad Management and / or client counterparts.
- Develop strong relationships with client counterpart and team leaders.
- Collaborate with Business Development in order to evaluate opportunities for risk, bandwidth, and project success.
- Facilitation of Quarterly Ops Review.
- Ensure that policies and procedures are being followed by project team.
- Ensure that all controls and processes (SSAE 16) are followed.

**Client Name:** *State of Minnesota*  
**Role(s) on Project:** *Service Delivery Manager*  
**Module(s):** *PeopleSoft FMS, HCM and OBIEE*  
**Environment:** *PeopleSoft v9.1*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *Georgia State Financing & Investment Commission (GSFIC)*  
**Role(s) on Project:** *Service Delivery Manager*  
**Module(s):** *PeopleSoft FMS*  
**Environment:** *PeopleSoft v.9.2*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *Sonoma County, CA*  
**Role(s) on Project:** *Service Delivery Manager*  
**Module(s):** *PeopleSoft FMS, Hyperion*  
**Environment:** *PeopleSoft v9.2*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *Indiana Public Retirement System (INPRS)*  
**Role(s) on Project:** *Service Delivery Manager*

- Manage and facilitate all Managed Services activities as well as ongoing client relationship related to Actuary reporting.
- Collaborate with INPRS Project Management on QA and UAT testing and issue resolution for Actuary Report.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.



**Client Name:** *CherryRoad Managed Services*

**Role(s) on Project:** *PMO*

- Develop standardized policies and processes to be followed by the managed services team.
- Work with PM / EM to improve project efficiency and communication.
- Report on project metrics to CherryRoad Management and / or client counterparts.
- Develop strong relationships with client counterpart and team leaders.
- Collaborate with Business Development in order to evaluate opportunities for risk, bandwidth, and project success.
- Facilitation of Quarterly Ops Review.
- Ensure that policies and procedures are being followed by project team.
- Ensure that all controls and processes (SSAE 16) are followed.

**Client Name:** *San Diego County of Education (SDCOE), CA*

**Role(s) on Project:** *Testing Manager / Service Delivery Manager*

**Module(s):** *HR, BN, BA, TL, AM, PY, GL, AP, AR, BI, PO, Banking*

**Environment:** *PeopleSoft v9.2 Implementation*

Service Delivery Manager for San Diego County of Education (SDCOE).

- Facilitated planning and management of the various testing cycles; System, Integration, UAT and Parallel for the District wide rollout of PeopleSoft.
- Manage and facilitate all Managed Services activities as well as ongoing client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *City & County of San Francisco Controller's Office (CCSF), CA*

**Role(s) on Project:** *Service Delivery Manager*

**Module(s):** *ELM*

**Environment:** *PeopleSoft v9.2 Implementation*

Service Delivery Manager for City and County of San Francisco as well as provide Quality Assurance and Project Management oversight for City and County of San Francisco Controller's Office ELM Implementation.

- Participate in team meetings in order to review and prioritize project tasks.
- Reviewed and updated project schedule based on changes to resource requirements and critical path.
- Liaison between client and implementation team for issue and risk management.
- Manage and facilitate all Managed Services activities as well as client relationship.
- Ensuring that quality services are delivered in regard to the agreed SLA.
- Providing detailed reports as per an agreed upon schedule, including management and account performance reports.
- Mitigating and solving escalations with urgency and determination.

**Client Name:** *Ramsey County, MN*

**Role(s) on Project:** *Project Manager*

**Module(s):** *SC*

**Environment:** *PeopleSoft v9.1 Implementation*

Project Manager for Ramsey County's Supplier Contract Management Implementation.

- Conducted team meetings in order to review and prioritize project tasks.
- Reviewed and updated project schedule based on changes to resource requirements and critical path.
- Identified corrective actions to address issues and project risks.



- Managed the prioritization of ongoing tasks, resource assignments and tracking against the project plan.

**Client Name:** *State of Minnesota*  
**Role(s) on Project:** *Project Manager*  
**Module(s):** *PO, ePro, SS, SC, eSup, Inventory, nVision Reporting*  
**Environment:** *PeopleSoft v9.1 Implementation*

Project Manager for Phase II of State of Minnesota's SWIFT Implementation focused on advanced procurement functionality and nVision reporting.

- Managed the full life cycle implementation including integration, data conversion, testing, and documentation deliverables across multiple State agencies.
- Conducted team meetings in order to review and prioritize project tasks with functional and technical resources.
- Reviewed and updated project schedule based on changes to resource requirements and critical path.
- Identified corrective actions to address issues and project risks.
- Reviewed changes in scope with client in order to identify required Change Requests.
- Produced and presented weekly metric reports to the State's Steering Committee.
- Built a long-term relationship with the client through open communication and proactive planning in order to catch up on late tasks and as well as provide visibility into upcoming tasks.
- Managed the prioritization of ongoing tasks, resource assignments and tracking against the project plan.

**Client Name:** *Cognizant*  
**Role(s) on Project:** *Functional Consultant*  
**Module(s):** *HR, Base Benefits, ePay, eProfile, eProfile Manager, ePerformance, eDevelopment, Payroll Interface, Absence Management, Connector for ADP, Track Global Assignments, Manage Competencies*  
**Environment:** *PeopleSoft v8.9 HCM Assessment*

Collaborated with TowersWatson to perform an HCM assessment and benchmark existing application landscape against the "best of breed" systems for one of the fastest growing consulting and outsourcing companies.

Cognizant's current employee strength is over 100,000 employees worldwide with expected rapid growth in the next 4-5 years, coupled with expansion in the global geographical footprint.

- Came to understand Cognizant's current usage patterns, interfaces and identified pain-points for PeopleSoft HCM (8.9) and ELM (9.0) in order to identify a solution that meets these requirements and is also scalable to cater to the expected growth the organization would witness in the next 5-7 years.
- Studied the key customizations, interfaces, and bolt-ons developed in PeopleSoft 8.9 and recommend a strategy to minimize them in the proposed solution.
- Explored opportunity to move as many non-PeopleSoft applications, currently being used, into the proposed solution by leveraging the features / functionalities available in PeopleSoft 9.1.
- Recommended how to enhance / reengineer some of the key people processes to make them seamless and efficient by leveraging on industry best practices.
- Provided an upgrade roadmap for PeopleSoft v8.9 to the recommended solution.

**Client Name:** *State of Minnesota*  
**Role(s) on Project:** *Project Team Lead*  
**Module(s):** *AP, AR, GL, PO, ePRO, SS, SC, eSUP, IN, CM, eSet, KK, AM, BI, PC, GM*  
**Environment:** *PeopleSoft v9.1 Implementation*

Managed consultant team of twenty as well as collaborated with client counterpart providing guidance to the client leads and SMEs on Statewide PeopleSoft Financials implementation for over 100 agencies.

- Managed the full life cycle implementation including integration, data conversion, testing, and documentation deliverables across multiple State agencies.



- Worked with business managers and Enterprise Readiness to ensure smooth transition from the "as is" to the "to be" business operating environment through communications, agency assignments and custom training.
- Conducted team meetings to review and prioritize project tasks with functional and technical resources.
- Reviewed and updated project schedule based on changes to resource requirements and critical path.
- Identified corrective actions to address issues and project risks.
- Reviewed changes in scope with client counterparts in order to identify required Change Requests.
- Produced and presented weekly metric reports to the State's Steering Committee.
- Built a long-term relationship with the client through open communication and proactive planning in order to catch up on late tasks and as well as provide visibility into upcoming tasks.
- Managed the prioritization of ongoing tasks, resource assignments and tracking against the projected plan.

**Client Name:** *Bay Area Rapid Transit District (BART)*  
**Role(s) on Project:** *Project Manager*  
**Module(s):** *BI, AR, CM, DM, GM, PC, CN, AM, PO, AP, ePro, SS, EX, GL, Planning, Budget*  
**Environment:** *PeopleSoft v9.0 Implementation*

Concurrent PeopleSoft Financials, OBIEE, Maximo, and Optram implementation as well as a PeopleSoft HCM upgrade to v9.0. Managed consultant team of seven as well as collaborated with client counterpart providing guidance to the client leads and SMEs.

- Managed the full life cycle implementation including integration, data conversion, testing, documentation, and training across the organization.
- Collaborated with concurrent implementations that included Oracle's OBIEE for reporting and KPIs, Bentley Solution's Optram for linear assets (train tracks), and IBM's Maximo for the maintenance and materials of trains.
- Collaborated with the change management team to assess the impact to the unions due to business process reengineering in order to produce communication plans, training plans, detailed procedures, job description updates, and an ROI analysis.
- Provided subject matter expertise and project oversight to the Human Capital Management Team during the upgrade to PeopleSoft v9.0 Human Resources, Base Benefits, Benefits Administration, Payroll, and Time and Labor; and served as the main integration interface across PeopleSoft HCM, Maximo, and PeopleSoft Financials.

**Client Name:** *Bay Area Rapid Transit District (BART)*  
**Role(s) on Project:** *Functional Consultant / Project Lead*  
**Module(s):** *eBen, Ben Admin, Human Resources*  
**Environment:** *PeopleSoft v8.8 Implementation*

PeopleSoft HCM implementation incorporating specific union rules related to benefits and time administration. Collaborated with client counterpart and provided guidance to SMEs.

- Module lead for full life cycle implementation including integration, data conversion, testing, documentation, and training across the organization.
- Delivered business requirements, integration, custom benefit solution based on union rules, integration to legacy financial and training systems, data conversion and testing.
- Collaborated with the change management team to assess the impact to the unions due to business process reengineering in order to produce communication plans, training plans, detailed procedures, job description updates, and an ROI analysis.

## Education

- Bachelor of Arts, Comparative Literature & Hispanic Studies, Brown University





7.1.3 **Describe in detail** the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

CherryRoad will assign a Contract Manager to represent and manage the entire account. The Contract Manager will serve as the Single Point of Contact (SPOC) for managing day-to-day activities of the engagement. The roles and responsibilities of the Contract Manager include, but are not limited to the following:

- Manage compliance with the scope and conditions from the contract.
- Provide a usage report for the quarterly sales reporting described in the in the Master Agreement Terms and Conditions.



## 6. Technical Response

*This section should constitute the Technical response of the proposal 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.*

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.*

*Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.*

CherryRoad's cloud solutions (IaaS and PaaS) were developed specifically for state and local government. We leveraged our platform and infrastructure experience attained by working with 14 states including the States of Oklahoma, Vermont, New Mexico, Tennessee, and Delaware. While working with hundreds of state agencies, CherryRoad learned that three components for state infrastructure and platform requirements stood out: **Security**, **Performance**, and a **Voice**. The requirements and liability of **Securing** PII has never been more important. The need for processing massing data transactions at the state level requires the highest **Performing** technology. And finally, ever-changing regulatory and compliance updates drive the need for states to have a **Voice** regarding their cloud requirements. CherryRoad saw that large public cloud providers could not provide solutions to government with these attributes. That's why CherryRoad built our IaaS and PaaS solutions specifically for state and local government. Our infrastructure, security, processes, and controls are designed to meet government compliance requirements and allows for clients to have a voice regarding what advancements and updates should be made in the future. Our solutions are designed from top to bottom for government, no labor or data information crosses U.S. borders, and all storage, monitoring, and access of data is confined within the U.S. Our services will provide the State with a unified environment providing flexible cloud infrastructure, a powerful standards-based platform, and a comprehensive portfolio of business applications, all on a subscription basis.

### Infrastructure as a Service (IaaS)

CherryRoad's Infrastructure as a Service (IaaS) offers a set of core infrastructure capabilities like elastic compute and storage to provide our clients the ability to run any workload in our cloud. Specifically, infrastructure services will include:

- *Compute Service* to leverage elastic compute capacity to address growing business needs.
- *Storage Service* to provide a secure, scalable, reliable, and simple storage solution to meet all of your enterprise needs.
- *Messaging Service* to leverage dynamic messaging capabilities for workflow agility.





## Platform as a Service (PaaS)

CherryRoad's PaaS solutions offer our clients the necessary tools help your organization innovate faster, increase productivity, and reduce costs. Specifically for developers, our offerings include:

- **Application Development** – In order to help our clients reduce the cost of developing, testing, and deploying applications CherryRoad utilizes our platform to roll out critical application development services. These service offerings allow our clients to develop and deploy nearly any type of application, including enterprise apps, lightweight container apps, web apps, mobile apps, and more. We utilize Oracle products that are based on prevailing Java standards, so development teams can use familiar architectures, utilities, and products.
- **Data Management** – Utilizing our Exadata systems, our clients can easily embark on a pure CherryRoad cloud or hybrid cloud strategy that spans on-premises databases as well as databases in the cloud.
- **Business Analytics** – Utilizing our platform, we can deliver Oracle's Business Analytics which provides an unmatched user experience with the ease and flexibility you need from your analytics system. Combine any data from any source for a complete view of your business.
- **Integration** – Integration Services simplify and accelerate integration of our cloud and your on-premises applications. With comprehensive cloud-based integration, you can maximize the value of data and create innovative services with greater agility and reduced risk.
- **Content and Process** – Organizations need cloud-based services that can blend content, people, processes, and communications as part of a cohesive workflow. The State can utilize a new generation of connected tools that drive meaningful collaboration and mobility.

We offer the State specialized public sector expertise and the knowledge of our staff, who have previously and successfully supported State initiatives. Our proposed services are the industry's broadest and most integrated public cloud, offering best-in-class functionality. Our services will provide the State with a unified environment providing flexible infrastructure, a powerful standards-based platform, and a comprehensive portfolio of business applications, all on a subscription basis.



## 8.1 (M) (E) Technical Requirements

*8.1.1 Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.*

### PaaS:

CherryRoad's cloud solution conforms with FIPS publication 199 for 3 levels of classifications of data, Low, Moderate, and High.

### IaaS:

CherryRoad's cloud solution conforms with FIPS publication 199 for 3 levels of classifications of data, Low, Moderate, and High.

*8.1.2 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 following characteristics, as defined in NIST Special Publication 800-145:*

*8.1.2.1 NIST Characteristic - On-Demand Self-Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.*

CherryRoad's cloud solution provides easy client enabled configuration via portal access to quickly provision CPU, Mem, Network, and security components.

*8.1.2.2 NIST Characteristic - Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided.*

CherryRoad's cloud solutions provide for multiple network access points. Private network utilizing Redundant MPLS, or Redundant internet public network utilizing VPN.

*8.1.2.3 NIST Characteristic - Resource Pooling: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met.*

CherryRoad's cloud solution provides adequate virtualized resource pooling to support on demand services for both Compute and Storage requirements. Capacity and performance management tools are used to manage resource allocations to ensure resource are added in a seamless fashion to ensure continued client growth and availability.



*8.1.2.4 NIST Characteristic - Rapid Elasticity: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met.*

CherryRoad's cloud solution provides a user access portal to self-provision compute resources as well as manage storage allocations. Once configuration parameters are entered, the service will configure and deliver the virtual machine ready for application or database configuration. Client can add or delete compute and storage resources at will.

*8.1.2.5 NIST Characteristic - Measured Service: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.*

CherryRoad's cloud solution provides internal billing capabilities to track changes and usage data. This data is then used to provide billing information via the portal and contains all details on usage and allocation.



8.1.3 Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

**IaaS (Infrastructure as a Service):** CherryRoad's cloud solution supports multiple government categories:

**PaaS (Platform as a Service):** CherryRoad's cloud solution supports multiple government categories:

**Education:**

- Analytics
  - Business Intelligence
  - Data Warehouse
- Database
  - Relational
  - SQL
- Development, Testing and Deployment
  - Containers
  - Services and APIs
  - Mobile
  - Internet of Things
  - Tools
  - Runtime environments
- Electronic Records Management
- E-Discovery
- GIS
- Integration (iPaaS)
- Open Source

**State and local government:**

- Analytics
  - Business Intelligence
  - Data Warehouse
- Database
  - Relational
  - SQL
- Development, Testing and Deployment
  - Containers
  - Services and APIs
  - Mobile



- Internet of Things
- Tools
- Runtime environments
- Electronic Records Management
- E-Discovery
- GIS
- Integration (iPaaS)
- Open Source

**Healthcare:**

- Analytics
  - Business Intelligence
  - Data Warehouse
- Database
  - Relational
  - SQL
- Development, Testing and Deployment
  - Containers
  - Services and APIs
  - Mobile
  - Internet of Things
  - Tools
  - Runtime environments
- Electronic Records Management
- E-Discovery
- GIS
- Integration (iPaaS)
- Open Source

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

CherryRoad complies with the requirements of attachments C&D.

*8.1.5 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.*

CherryRoad is offering IaaS and PaaS on a private cloud as outlined in scope of services in attachment D.



## 8.2 (E) Subcontractors

*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.*

CherryRoad will provide all Cloud Solutions directly. We do not plan to use sub-contractors to deliver services.

*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.*

CherryRoad will provide all Cloud Solutions directly. We do not plan to use sub-contractors to deliver services.

*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.*

CherryRoad will provide all Cloud Solutions directly. We do not plan to use sub-contractors to deliver services.

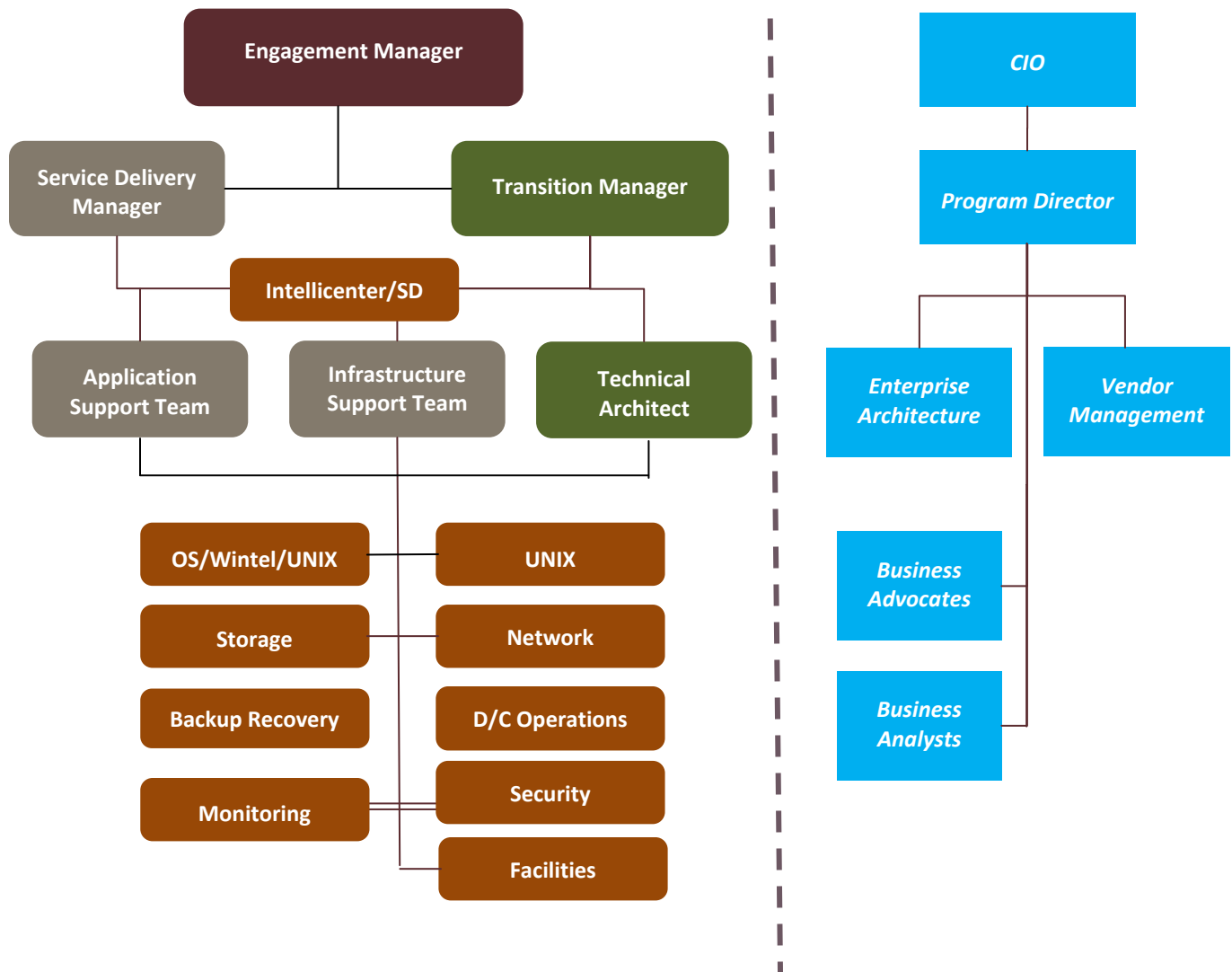


### 8.3 (E) Working with Purchasing Entities

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.

CherryRoad's Account governance team will provide the services necessary to support all purchasing agents' requirements on a peer-to-peer level, from executive level to business analyst.





### Account Executive (AE):

Your Account Executive (AE) is responsible for all contractual responsibilities. The AE represents the highest level of escalation outside of CherryRoad executive management. He has the authority and the experience to address any and all concerns the purchasing agent may encounter. The AE works closely with both the Transition Manager who provides initial technical planning and support serviced during the initial build and on-boarding process and Service Delivery Manager who provides all the day to day logistical support to the purchasing agents.

### Transition Manager (TM)

Your Transition Manager (TM) is responsible for ensuring all contractual build and migration activity is planned and scheduled according to client requirements. The TM is also responsible for working with the AE to ensure all purchasing agent requirements are understood to ensure all design and build tasks are scheduled and accounted for. Once complete the TM will work with the SDM to ensure all day-to-day governance process and procedures are in place for a seamless integration into steady state.

### Service Delivery Manager (SDM):

Your Service Delivery Manager (SDM) works directly with your purchasing agents to ensure their needs are met. In the specific event of a security breach, the SDM will work directly with the CherryRoad IntelliCenter to ensure tickets are generated and the appropriate technical communication plans are enacted. The SDM will work with CherryRoad Security and Delivery engineers to isolate and report of the incident to the effected purchasing agent.

*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.*

CherryRoad does not permit adware or any form of marketing on our system. We will fully enforce our user acceptance policy and utilize tools to monitor and detect such activity.

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

CherryRoad's cloud infrastructure allows for clients to self-provision systems according to their requirements which includes development, test, and development systems.

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

CherryRoad web sites and computer applications are accessible to people with disabilities and will comply with participating clients' accessibility policies and with the Americans with Disabilities Act, as applicable





*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 minimum.*

CherryRoad supported applications will support vendor supported Web Browsers.

*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.*

Through all new client on-boarding activities, CherryRoad will work with each client to determine the proper Service Levels (if outside our standard) and all requirements related to privacy and security. These requirements will be assessed and represented in the initial configuration of the service provided. On a monthly basis, all service levels are reviewed and will be discussed to ensure compliance obligations are being met. In the event a change is needed, the monthly review meetings will be the vehicle to institute these types of changes.

*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.*

As part of each project and/or on-boarding initiative, a project schedule will be developed collaboratively with the client. This plan typically will consist of a transition period which provides for the on-boarding and initial configuration onto the respective cloud service (i.e., IaaS or PaaS). The initial configuration will directly impact the associated timelines. Once the environments are configured and ready for use, the client will provide the initial testing. Both the IaaS and PaaS configurations are then moved into Steady State and then are governed by the agreed upon Service Levels. Individual development and solution testing will be the responsibility of the client and governed by the client's respective project schedule.



## 8.4 (E) Customer Service

8.4.1 Offeror must describe how it 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).

The CherryRoad user experience begins with your SDM and Account Executive. Together they are responsible for delivery, monitoring and reporting on our service requirements and SLA targets. Every level of CherryRoad's service model is aware and strives to not only meet these objectives but to exceed them at all levels.

Your service delivery manager is your everyday contact, ensuring that SLAs are being met and tickets are receiving the attention they require. Your SDM will hold weekly meeting with you to review ticket information as well as SLA performance.

Monthly meetings are held to ensure appropriate planning initiatives are covered and review SLA performance for the month.

Your SDM and AE will hold quarterly meetings to review the strategic components of the relationship. Discussing growth opportunities, escalations, and go forward plans.

Escalation can be accomplished in a number of ways:

- Our Intellicenter is staffed 7x24x365. Here purchasing agents can open a ticket of escalation for which will be directed to both your SDM and AE. Staff will track these tickets to ensure a rapid response and direct call back is initiated to quickly address any issue.
- Your SDM is available 7x24x365 should you require specific assistance.
- Your AE is also available to both address any issue and involve corporate resources if required.

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.

CherryRoad will provide upon completion of agreement of services the following account support personnel.

- Account Executive responsible for account relationship and overall delivery to contract and support agreements.
- Service Delivery Manager responsible for day-to-day operational delivery, SLA reporting, ticket management and operational escalations.



*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.*

- CherryRoad Intellicenter personnel provide 7x24x365 coverage and our Service Now ticket system can accommodate ticket origination and updates via email or network access.

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

- CherryRoad personnel will respond to inquiries within 24 hours.

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

- CherryRoad technical services can provide design support services at purchasing agents request.

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

- Cherry Road technical services can provide installation services for all applicable categories.



## 8.5 (E) Security of Information

*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.*

Security is a process and not a single product as such CherryRoad takes client data protection seriously and our processes and offerings are always under improvement and tightening as best practices evolve. Some of the services provided today are:

- Anti-virus on all systems – Required
- Host Based IDS – Required
- Firewalls – Required
- Network IDS - Required
- Physical Network separation – Required
- SIEM system monitoring to monitor all vital infrastructures.
- All data at rest is encrypted.
- All offsite tape data is encrypted.
- All user accounts are individual and subscribe to least privilege.
- Data Center physical security requires badged user 24x7x365 guarded.
- All equipment is physically secured in locked cages on datacenter floor.
- VPN encrypted access with two factor authentication.

Separation of administrative duties is also employed to ensure that no one individual can access and change customer data.

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

CherryRoad infrastructure standards are based on industry best practices and are constantly under review. We monitor for changes in laws and privacy movements and will work with individual purchasing agents to address emerging requirements and changes required to meet those commitments.

*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.*

CherryRoad offers multiple solutions to integrate and manage purchasing agents access requirements and security (AD, Local, Client AD, LDAP). Our engineers will meet with purchasing entities to discuss current capabilities already in place and leverage CherryRoad capabilities to provide solutions acceptable for their individual case. In some cases, a specific solution will be developed on a case-by-case basis depending on requirements.



## 8.6 (E) Privacy and Security

*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.*

CherryRoad is committed to providing safe and secure systems using industry best practices. Our policy and practice of constant improvement is designed to ensure that industry best practices are implemented at all times.

*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.*

CherryRoad managed systems undergo annual audits to review adherence to industry best practices. CherryRoad has successfully completed the following outside attestations.

- HIPPA
- SSAE-16

CherryRoad is currently engaged on the following certifications for current year 2016.

- PCI
- NIST 800-53
- CSA
- 270001

*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.*

CherryRoad is committed to providing safe and secure systems using industry best practices. Our policy and practice of constant improvement is designed to ensure that industry best practices are implemented at all times.

Some of the services provided today are:

- Anti-virus is run on all systems and maintained by our operations staff.
- Host-based IDS is run on all systems and maintained by our operations staff.
- Firewalls protect the outside perimeter for both internet and private networks. They provide for segregation of data and a choke point for unauthorized data access. The CherryRoad network team supports these devices and all security data is reviewed to detect any unwanted activity.
- Network IDS is employed to not only detect but to deter unwanted activity to protect the integrity and availability of the data transporting over CherryRoad networks.
- Physical Network separation of all client data to ensure privacy and security.



- SIEM system monitoring to monitor all vital infrastructures.
- All data at rest is encrypted to ensure privacy while at rest.
- All offsite tape data is encrypted to ensure privacy from outside threats.
- All user accounts are individual and subscribe to least privilege.
- DataCenter physical security requires badged user 24x7x365 guarded to thwart any unauthorized access to infrastructure or media containing client data.
- All equipment is physically secured in locked cages on datacenter floor.
- VPN encrypted access with two factor authentication.
- All supported applications, databases and network are hardened according to industry best practices and validated via annual independent audits:
  - SSAE-16
  - HIPPA
  - NIST 800-53
  - PCI
  - 27001
  - CSA

*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).*

CherryRoad currently employs the following policies and standards to ensure data confidentiality.

- Access credentials utilize best practice of least privileged.
- Every administrative user must have their owned named account.
- Remote Administrator Access Process: Requires two factor authentication and secure VPN with encryption.
- Password Administration policy
- PC acceptable use policy/
- User Administration policy
- Employment termination and account removal process.

CherryRoad and industry best practice require that all user access is reviewed on a regular basis. Access credentials are locked out after 5 unsuccessful attempts. CherryRoad administrative user account access is reviewable annually and is restricted to least privilege.

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

CherryRoad managed systems undergo annual audits to review adherence to industry best practices. CherryRoad has successfully completed the following outside attestations.

- HIPPA
- SSAE-16



CherryRoad is currently engaged on the following certifications for current year 2016.

- PCI
- NIST 800-53
- CSA
- 270001

*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.*

CherryRoad managed systems undergo annual audits to review adherence to industry best practices. CherryRoad has successfully completed the following outside attestations.

- HIPPA
- SSAE-16

CherryRoad is currently engaged on the following certifications for current year 2016.

- PCI
- NIST 800-53
- CSA
- 270001

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

All cloud systems are deployed in a customer specific VLANs. VLANs from different customers are firewalled. Customer VMs are dedicated and are not accessible by other entities. SAAS applications use application level security to ensure that customer data is compartmentalized and not shared.

*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.*

CherryRoad security incident process requires 72-hour notification of a confirmed security breach. Process includes incident investigation, risk and impact analysis in accordance with applicable laws and categorization types. This would include datacenter security, vendor product security vulnerability, or security incident that affects data integrity or availability.



*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.*

CherryRoad isolates customers to unique firewalled VLANs. Shared infrastructure is zoned and hardened to prevent data leakage. This hardening includes shared Exadata infrastructure, SNMP monitoring, and virtualized hypervisors.

Physical access requires passing through multiple layers of security to get to CherryRoad's hosted infrastructure. This includes a guarded entrance, the requirement of a security badge and a biometric scan.

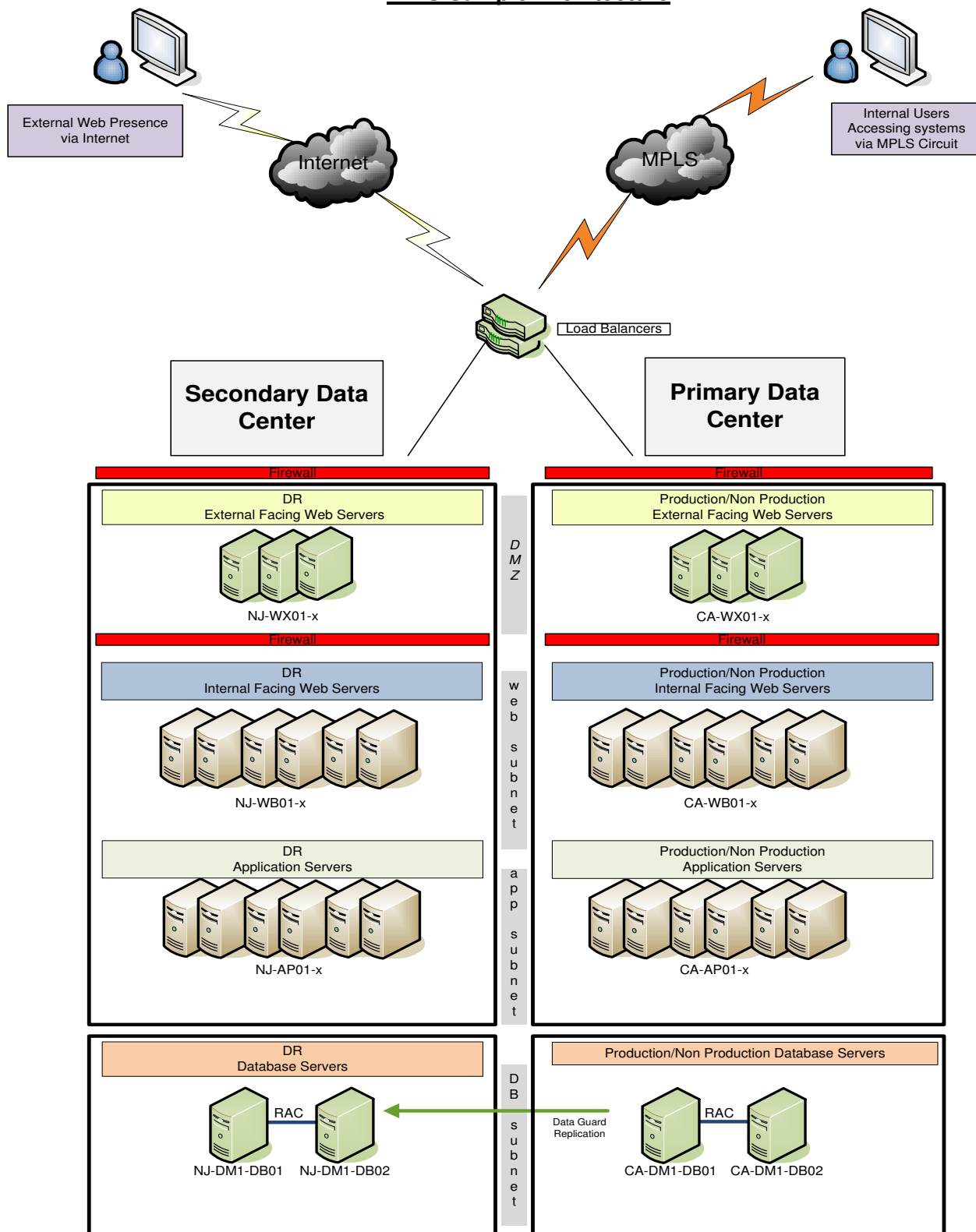
*8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).*

Please see the graphic on the following page:



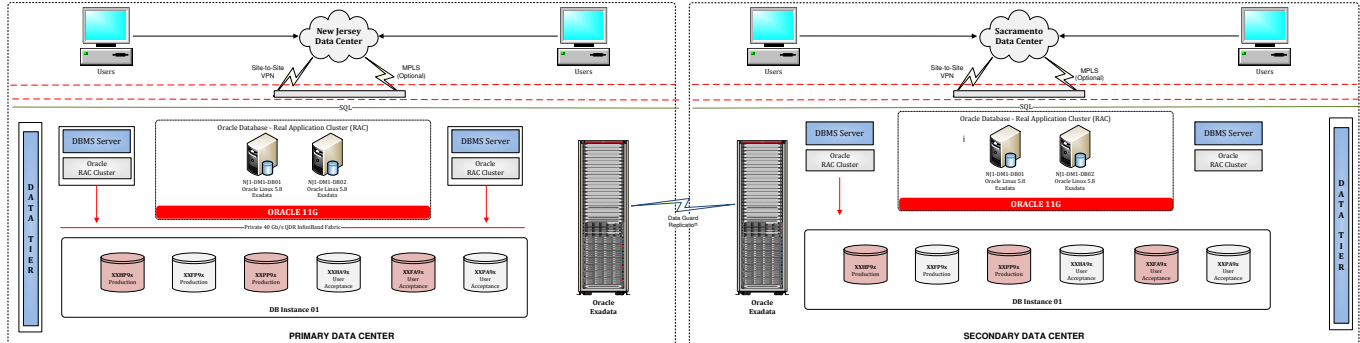


### IAAS Sample Architecture





### PAAS Sample 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.

CherryRoad's background check process is two pronged. First, we notify candidates via the Employment Application during the interview process, that background checks will occur as a requirement of employment with CherryRoad. Secondly, once a decision to make an offer of employment is finalized, the candidate receives an Offer of Employment letter, which incorporates information regarding the background check and a statement that employment is contingent upon several conditions, one of which is a satisfactory background check. The candidate is supplied with the appropriate acknowledgments and forms, and once CherryRoad receives the candidate's completed, signed authorization, the background check is executed.

The background check is performed by an outside vendor, ClearStar Background. Our standard check includes: Federal District Court, National Criminal, Local Counties if required, Social Security scan, National State Sex Offenders Registries, and finally the OIG Exclusions List search.

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.

CherryRoad is aligned to NIST standards. Data at rest and in transit are encrypted using AES encryption or TLS encryption for web traffic

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.

CherryRoad will notify the purchasing agent in the event of any security breach within 72 hours



## 8.7 (E) Migration and Redeployment Plan

*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.*

Upon termination or expiration of this Agreement for any reason, CherryRoad will work with each purchasing entity on a disentanglement plan and will ensure that all data components remain secured until data transition and purchasing entity acceptance. CherryRoad will also ensure that all remaining copies of data are erased/deleted upon data movement and a release to erase data has been secured from the purchasing agent.

*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.*

Upon termination or expiration of this Agreement for any reason, CherryRoad will work with each purchasing entity on a disentanglement plan and will ensure that all purchasing data is returned. CherryRoad SLA timelines can be defined with purchasing agents requirements. In practice, CherryRoad may deploy a number of technologies to return purchasing agent data. These mechanisms may include:

- Replication of client data.
- Encrypted drives.
- SFT Transfer.

CherryRoad will work with purchasing agents to address specific needs and capabilities to ensure smooth transition of purchasing agent data.



## 8.8 (E) Service or Data Recovery

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).

- a. If extended downtime is caused by an issue at the primary CherryRoad data center. CherryRoad will invoke our disaster recovery plan.
- b. CherryRoad would restore from the last viable backup in the case of and data loss.
- c. CherryRoad will work with the State to develop a Business Continuity Plan (BCP). This BCP would be invoked in the case of a business failure.
- d. RPO and RTO are determined by contracted SLA. CherryRoad has the ability to provide up to a 15 min RPO and 2 hour RTO.

8.8.2 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.

- a. CherryRoad utilizes a Commvault Simpana infrastructure to perform nightly backups. Backups are stored on tape and/or EMC Data Domain devices and either shipped offsite or replicated to a secondary data center. Typical backup retention is as follows:
  - Nightly Backups – 2 weeks
  - Weekly backups – 1 month
  - Monthly backups – 1 year
- b. Virtual server image backups are performed via Veeam Backup and Replication.
- c. Depending on contracted SLA, backups are stored on either tape or EMC DataDomain devices. If tape backup is utilized, tapes are moved offsite on a weekly basis.
- d. CherryRoad operates two data centers in the US. One is in Totowa, NJ and one is in Sacramento, CA.



## 8.9 (E) Data Protection

*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.*

CherryRoad deploys a number of encryption technologies to secure purchasing agent data. Technologies include:

### Data in Transit:

- TLS / IPsec
- Firewalls/DMZ
- IDS/HPS
- Private network (MPLS)
- Encrypted drives. (For transition data transport)

### Data at Rest:

- Storage encryption.
- Offsite encrypted tapes.

*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.*

CherryRoad will sign relevant and applicable Business Associate Agreements or any other agreement that may be necessary to protect data with 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.*

CherryRoad will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. CherryRoad will not use the government data or government related data for any other purpose including but not limited to data mining. CherryRoad or its subcontractors shall not resell or otherwise redistribute information gained from its access to data received as a result of this RFP.



## 8.10 (E) Service Level Agreements

*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.*

CherryRoad believes not all SLAs fit all client needs and will work with each purchasing agent to develop agreeable SLAs and measurements. Below is a sample SLA report.

*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.*

SLA Ref #	Service Area	Service	Target Service Level
1.a	Disaster Recovery	Production Restoration	RTO <= 48 hours RPO <= 24 hours
1.b	Disaster Recovery	Non-production Restoration	RTO <=4 business days RPO <= 24 Hours
2.a	Help Desk Ticket Resolution Time	Priority 1	Target Resolution in <= 2 hours
2.b	Help Desk Ticket Resolution Time	Priority 2	Target Resolution in <= 4 hours
2.c	Help Desk Ticket Resolution Time	Priority 3	Target Resolution in <= 8 hours
2.d	Help Desk Ticket Resolution Time	Priority 4	Target Resolution in <= 24 hours
2.e	Help Desk Ticket Resolution Time	Priority 5	Target Resolution in <= 72 hours
3.a	Help Desk Ticket Response Time	Priority 1	Response in <= 15 minutes
3.b	Help Desk Ticket Response Time	Priority 2	Response in <= 15 minutes
3.c	Help Desk Ticket Response Time	Priority 3	Response in <= 30 minutes
3.d	Help Desk Ticket Response Time	Priority 4	Response in <= 30 minutes
3.e	Help Desk Ticket Response Time	Priority 5	Response in <= 72 hours
4	Data Backup and Restoration	Backup Success Rate	>=99.0 % Success
5	Data Restoration and Refresh	Restoration Time	To Be Determined
6	System Refreshes	Non-Production	<= 48 hours
7.a	Security	Compliance	99% Compliance
7.b	Security	Annual Review	>-98.00%
7.c	Security	Physical Security	>-98.00%



SLA Ref #	Service Area	Service	Target Service Level
7.e	Security	Fire Detection and Prevention	>-98.00%
8	System Availability	Production Uptime	>-99.95%

### Ticket Priority Determination

The priority of all new incidents logged for MSC support will be assigned a level based on the entered Impact and Urgency. The Impact and Urgency is set by reporting user, and be manually adjusted by MSC staff with concurrence from Miami Children's Hospital. In general, the predefined definition of each Priority Level is as follows:

Priority	Definition / Description	Environment Impacted	Work Schedule and Status Communication
1	Critical Service Unavailable	Production	24 hrs/day x 365 days/year Status updates provided <b>every 2 hours</b> on a 24x365 basis until issue resolved or reprioritized.
2	Essential Service Severely Halted or Impacted, No Workaround Available	Production	16 hrs/day x Monday-Sunday excl. Holidays Status updates provided <b>every 4 hours</b> until issue resolved or reprioritized.
3	Service Impacted or Degraded, No Workaround Available	Production, Training	16 hrs/day x Monday-Friday excl. Holidays Status updates provided <b>daily</b> until issue resolved or reprioritized.
4	Service Impacted or Degraded but workaround is available to fully mitigate impact.	All Hosted Environments (Production/Non-Production)	10 hrs/day x Monday-Friday excl. Holidays Status updates provided <b>weekly</b> until issue resolved or reprioritized.
5	Informational OR Enhancement request OR Monitor status to ensure stability OR Work Request/Infrastructure Change	All Hosted Environments (Production/Non-Production)	8 hrs/day x Monday-Friday excl. Holidays Status updates provided <b>weekly</b> until issue resolved or reprioritized



### 8.11 (E) Data Disposal

*Specify your data disposal procedures and policies and destruction confirmation process.*

All CherryRoad storage arrays and portable storage utilize AES encryption; this ensures that data is protected if drives are obtained by a third party. If equipment is retired or malfunctions the devices are wiped of data and where possible destroyed by a third party.





## 8.12 (E) Performance Measures and Reporting

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.

Through the use of redundancy at every hardware layer, CherryRoad has the ability to offer a 99.99% availability guarantee. This can be included in the SLA agreement with the State.

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

CherryRoad's standard uptime and related SLAs are included below:

SLA Ref #	Service Area	Service	Target Service Level
1.a	Disaster Recovery	Production Restoration	RTO <= 48 hours RPO <= 24 hours
1.b	Disaster Recovery	Non-production Restoration	RTO <=4 business days RPO <= 24 Hours
4	Data Backup and Restoration	Backup Success Rate	>=99.0 % Success
5	Data Restoration and Refresh	Restoration Time	To Be Determined
6	System Refreshes	Non-Production	<= 48 hours
8	System Availability	Production Uptime	>-99.95%

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.

CherryRoad provides a 24x7x365 Help Desk with multiple options for an entity to contact our team to log an incident. This includes:

### Toll Free Number

A Toll-Free Number is available to contact the Help Desk for Help Desk Tickets or to report new issues. Based on the prompt options, the caller will be routed to the appropriate skill set based on the reason for the call. The Call Center is available 24x7x365.

Toll Free Number: 1-877-9-CRT-FIX (1-877-927-8349)

### Help Desk Email

An email will be established for each entity utilizing the following structure [crtfixxxx@cherryroad.com](mailto:crtfixxxx@cherryroad.com).



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

As part of the statement of work (SOW) process CherryRoad will work with the State to determine the appropriate remedy in the event an SLA metric is not met during the agreed upon measurement period. Typically, measurements are done over the course of a month and tracked within our ServiceNow ticketing system. In some instances a monthly credit can be established as a remedy in the event a metric is missed.

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

CherryRoad has a standard maintenance window of 3 am – 11 am EST every Saturday. Clients are notified via email of all scheduled maintenance at least 72 hours in advance.

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

As part of the statement of work (SOW) process CherryRoad will work with the State to determine the appropriate remedy in the event an SLA metric is not met during the agreed upon measurement period. Typically, measurements are done over the course of a month and tracked within our ServiceNow ticketing system. In some instances, a monthly credit can be established as a remedy in the event a metric is missed.

*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.*

CherryRoad performance reports are derived from real-time resources and will be available over the client portal.

### **Sample Performance Management Report**

CherryRoad has provided our Sample Performance Management Report as a separate attachment.

Please see:

- **Technical Response – 8.12.7 – CherryRoad Sample Performance Management Report.pdf**

January 2016

CHERRYROAD  
MANAGED  
SERVICES  
CENTER

## PERFORMANCE MANAGEMENT REPORT – PURCHASING AGENT

Bridging the gap from vision to solution

### Document Revision History

Date	Version	Description	Author
02/01/2016	1	Version 1	

### Reviewers

Name	Role	Attended Review?
	Purchasing Agent	NA
	Purchasing Agent	NA
	Purchasing Agent	NA
	CherryRoad	NA
	CherryRoad	NA
	CherryRoad	NA



## Table of Contents

<b>Document Revision History .....</b>	<b>ii</b>
<b>Objective .....</b>	<b>1</b>
<b>Scope .....</b>	<b>1</b>
Help Desk .....	1
Ticket Priority Determination .....	3
<b>Key Assumptions .....</b>	<b>4</b>
Help Desk .....	5
All Issues.....	6
<b>Performance and Capacity Metrics .....</b>	<b>10</b>

## Objective

The objective of the Purchasing Agent Performance Management Report is to present relevant information and results of the agreed upon service levels as defined in the Purchasing Agent-CherryRoad contract Statement of Work (SOW).

## Scope

The scope of the Purchasing Agent Performance Management Report includes compliance targets within the Help Desk service areas.

## Help Desk

The table below is from the Purchasing Agent – CherryRoad Statement of Work Table 6.6: Implementation Hosting SLAs. It defines the Implementation Hosting Service Level Agreements (SLAs), the method for monitoring the SLAs, and the Remedy should CherryRoad fail to meet a SLA.

SLA Ref #	Service Area	Service	Target Service Level	Credit *
1.a	Disaster Recovery	Production Restoration	RTO <= 48 hours RPO <= 24 hours	20% of monthly hosting fee.
1.b	Disaster Recovery	Non-production Restoration	RTO <=4 business days RPO <= 24 Hours	10% of monthly hosting fee
2.a	Help Desk Ticket Resolution Time	Priority 1	Target Resolution in <= 2 hours	N/A
2.b	Help Desk Ticket Resolution Time	Priority 2	Target Resolution in <= 4 hours	N/A
2.c	Help Desk Ticket Resolution Time	Priority 3	Target Resolution in <= 8 hours	N/A
2.d	Help Desk Ticket Resolution Time	Priority 4	Target Resolution in <= 24 hours	N/A
2.e	Help Desk Ticket Resolution Time	Priority 5	Target Resolution in <= 72 hours	N/A
3.a	Help Desk Ticket Response Time	Priority 1	Response in <= 15 minutes	5% of monthly hosting fee

## Performance Management Report January 2016

SLA Ref #	Service Area	Service	Target Service Level	Credit *
3.b	Help Desk Ticket Response Time	Priority 2	Response in <= 15 minutes	N/A
3.c	Help Desk Ticket Response Time	Priority 3	Response in <= 30 minutes	N/A
3.d	Help Desk Ticket Response Time	Priority 4	Response in <= 30 minutes	N/A
3.e	Help Desk Ticket Response Time	Priority 5	Response in <= 72 hours	N/A
4	Data Backup and Restoration	Backup Success Rate	>=99.0 % Success	5% of monthly hosting fee
5	Data Restoration and Refresh	Restoration Time	To Be Determined	N/A
6	System Refreshes	Non-Production	<= 48 hours	N/A
7.a	Security	Compliance	99% Compliance	N/A
7.b	Security	Annual Review	>-98.00%	N/A
7.c	Security	Physical Security	>-98.00%	N/A
7.e	Security	Fire Detection and Prevention	>-98.00%	N/A
8	System Availability	Production Uptime	>-99.95%	

### Ticket Priority Determination

The priority of all new incidents logged for MSC support will be assigned a level based on the entered Impact and Urgency. The Impact and Urgency is set by reporting user, and be manually adjusted by MSC staff with concurrence from Purchasing Agent. In general, the predefined definition of each Priority Level is as follows:

Priority	Definition / Description	Environment Impacted	Work Schedule and Status Communication
<b>1</b>	Critical Service Unavailable	Production	24 hrs/day x 365 days/year Status updates provided <b>every 2 hours</b> on a 24x365 basis until issue resolved or reprioritized.
<b>2</b>	Essential Service Severely Halted or Impacted, No Workaround Available	Production	16 hrs/day x Monday-Sunday excl. Holidays Status updates provided every <b>4 hours</b> until issue resolved or reprioritized.
<b>3</b>	Service Impacted or Degraded, No Workaround Available	Production, Training	16 hrs/day x Monday-Friday excl. Holidays Status updates provided <b>daily</b> until issue resolved or reprioritized.
<b>4</b>	Service Impacted or Degraded but workaround is available to fully mitigate impact.	All Hosted Environments (Production/Non-Production)	10 hrs/day x Monday-Friday excl. Holidays Status updates provided <b>weekly</b> until issue resolved or reprioritized.
<b>5</b>	Informational OR Enhancement request OR Monitor status to ensure stability OR Work Request/Infrastructure Change	All Hosted Environments (Production/Non-Production)	8 hrs/day x Monday-Friday excl. Holidays Status updates provided <b>weekly</b> until issue resolved or reprioritized

\*\* Outside of normal business hours, Monday – Friday, 8 am – 6 pm PST, in order to get the response time listed in the SLA chart above, new incidents should be logged via the Managed Services ticketing system, Service Now except for **Priority 1** issues, which should be logged via the Managed Services toll free number, 1-877-9-CRTFIX.



## Key Assumptions

The list below itemizes the key assumptions made in the collection, collation, or conclusions within the information presented in the Performance Management Report. The assumptions communicate how (and sometimes why) calculations were made so the reader is able to validate and/or reproduce the results.

Any change to these assumptions could impact one or more results contained within the report.

1. Help Desk service area:
  - a. Total Opened counts include all tickets opened (created) in the applicable reporting period, excluding duplicates.
  - b. Total Closed counts include all tickets closed (resolved and closed) in the applicable reporting period, excluding duplicates, and which were opened since CherryRoad services were in effect.
  - c. Response time is determined by the system notification electronically generated when the ticket was opened (created).
  - d. Response and Resolution counts only include tickets worked by CherryRoad resources and fall within CherryRoad scope and responsibilities.

## Help Desk

For each priority level, the number of new Help Desk Tickets opened, number of Help Desk Tickets closed, and number of open Help Desk Tickets remaining.

Priority	Assigned	Waiting for Customer Input	Waiting Client Review/Test	Resolved	Closed	Grand Total
1 Production Down					2	2
2 Essential Process Halted					21	21
3 Rpt/Process Not functioning - workaround NOT avail				1	24	25
4 Rpt/Process Not functioning - workaround avail	1	2		4	13	20
5 Informational	1	3	3	6	33	46
<b>Grand Total</b>	<b>2</b>	<b>5</b>	<b>3</b>	<b>11</b>	<b>93</b>	<b>114</b>

## All Issues

A listing of all open Help Desk Tickets as of this report.

Number	Incident state	Priority	Assigned To	Short Description	Opened	Caller
INC1883715	Waiting Client Review/Test	5 Informational		clear and activate the publication and subscription of IB in mcf92.	2016/02/10 07:13:28	
INC1884494	Waiting for Customer Input	5 Informational		Ports	2016/02/10 15:54:03	
INC1884499	Waiting for Customer Input	4 Rpt/Process Not functioning - workaround avail		Database access	2016/02/10 15:57:03	
INC1885094	Waiting Client Review/Test	5 Informational		JRNL upload template from mcf92instance	2016/02/11 08:50:08	
INC1891774	Waiting Client Review/Test	5 Informational		Current Image for PeopleSoft HCM	2016/02/18 09:33:21	
INC1892225	Assigned	4 Rpt/Process Not functioning - workaround avail		Installation of Image 16 in Finance	2016/02/18 14:27:12	
INC1894541	Waiting for Customer Input	5 Informational		We need to access MCFC92 (Conversion) environment from Mobile device	2016/02/22 03:10:59	
INC1895698	Assigned	5 Informational		Regarding Calirvia Integration with Peoplesoft	2016/02/22 21:58:18	

A listing of all Help Desk Tickets that were resolved during the month of this report.

Number	Incident state	Priority	Assigned To	Short Description	Opened	Caller	Resolved Date
INC1828919	Closed	4 Rpt/Process Not functioning - workaround avail		Access to CherryRoad Terminal Server and PeopleSoft Instances	2015/12/11 12:38:08		2016/01/07

## Performance Management Report January 2016

Number	Incident state	Priority	Assigned To	Short Description	Opened	Caller	Resolved Date
INC1840921	Closed	2 Essential Process Halted		NVision not installed	2015/12/28 09:59:48		2016/01/22
INC1843055	Closed	5 Informational		Terminal Server and Database access to New Team Members	2015/12/30 13:59:57		2016/01/06
INC1847119	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Access to CherryRoad Terminal Server	2016/01/05 13:50:23		2016/01/07
INC1848754	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Search option is not working as expected in Finance.	2016/01/06 16:46:33		2016/01/19
INC1849218	Closed	3 Rpt/Process Not functioning - workaround NOT avail		We are not having access to the folder where the trace files are created	2016/01/07 08:04:11		2016/01/11
INC1849225	Closed	5 Informational		Bouncing the application server	2016/01/07 08:08:36		2016/01/08
INC1849226	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Not having access to the report repository location where reports are created (w	2016/01/07 08:09:42		2016/01/11
INC1849372	Closed	5 Informational		Please install the SQR pluggin for Notepad++ on the terminal server	2016/01/07 10:00:03		2016/01/15
INC1849494	Closed	2 Essential Process Halted		On demand maintainance process erred out. Please see the attachment.	2016/01/07 11:01:43		2016/01/08
INC1849769	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Delete Employee profiles from UAT and TST environemnts except the super users.	2016/01/07 13:56:06		2016/01/11
INC1850794	Closed	4 Rpt/Process Not functioning - workaround avail		Push Notification configuration is incomplete	2016/01/08 12:43:45		2016/01/11
INC1852424	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Offshore team is not able to access Terminal Server	2016/01/11 09:14:42		2016/01/20
INC1853241	Closed	2 Essential Process Halted		Write access for Finance DEMO environemnt	2016/01/11 16:44:26		2016/01/13
INC1853779	Closed	5 Informational		Is PeopleSoft and database on Windows NT or Unix?	2016/01/12 09:17:40		2016/01/13

## Performance Management Report January 2016

Number	Incident state	Priority	Assigned To	Short Description	Opened	Caller	Resolved Date
INC1853780	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Excel to CI	2016/01/12 09:18:39		2016/01/12
INC1854430	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Anthony Kodwiw does not have access to database. Can you please help with that.	2016/01/12 15:37:00		2016/01/19
INC1856760	Closed	5 Informational		Access Removal - Madhu Ravela	2016/01/14 14:39:57		2016/01/15
INC1856900	Closed	4 Rpt/Process Not functioning - workaround avail		Workflow is not triggering the Emails	2016/01/14 16:24:11		2016/01/21
INC1857691	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Files are not getting generated in View Log/Trace process details	2016/01/15 12:35:34		2016/01/26
INC1858898	Closed	2 Essential Process Halted		Hi, need access and path to upload files in <a href="https://mfc92.hosted.cherryroad.com">https://mfc92.hosted.cherryroad.com</a>	2016/01/18 00:36:17		2016/01/22
INC1859903	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Attachments link is not working for Travel Authorization and Expense Reports.	2016/01/18 16:55:08		2016/01/21
INC1860401	Closed	4 Rpt/Process Not functioning - workaround avail		What is the image version of the current peoplesoft package we are using?	2016/01/19 07:25:43		2016/01/20
INC1860593	Closed	5 Informational		RDP is not working for user apatil.	2016/01/19 09:50:43		2016/01/19
INC1860603	Closed	5 Informational		RDP is not working on system. Need your help to resolve it.	2016/01/19 09:53:48		2016/01/19
INC1860622	Closed	5 Informational		I am not able to login to remote desktop in my citrix account	2016/01/19 09:59:51		2016/01/20
INC1860630	Closed	5 Informational		Hi Shruti Lahothy is not able to login to Citrix remote desktop.	2016/01/19 10:02:38		2016/01/20
INC1860634	Closed	5 Informational		The remote session disconnected because the license store creation failed.	2016/01/19 10:05:28		2016/01/19
INC1860642	Closed	5 Informational		This SR is created as a placeholder for the refreshes that we are going to need.	2016/01/19 10:08:34		2016/01/19

## Performance Management Report January 2016

Number	Incident state	Priority	Assigned To	Short Description	Opened	Caller	Resolved Date
INC1860655	Closed	5 Informational		MCFC92 instance is working very slow for all offshore members. Also App designer	2016/01/19 10:15:16		2016/01/20
INC1860786	Closed	2 Essential Process Halted		Was there any changes done in the MCFT92 environment?	2016/01/19 11:21:04		2016/01/20
INC1861881	Closed	5 Informational		Regarding login Issue in MCHC92 PIA	2016/01/20 07:53:42		2016/01/20
INC1861911	Closed	2 Essential Process Halted		All the environments are very slow, not able to login.	2016/01/20 08:18:28		2016/01/20
INC1863482	Closed	2 Essential Process Halted		Access to delete trace file from all the environemnts	2016/01/21 10:57:59		2016/01/22
INC1864755	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Need delete access for trace files for below folder	2016/01/22 09:16:35		2016/01/27
INC1864758	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Access to CherryRoad environment and Database for HCM	2016/01/22 09:17:21		2016/01/26
INC1865873	Closed	2 Essential Process Halted		Not able to login to CherryRoad Environment	2016/01/24 09:06:09		2016/01/24
INC1866683	Closed	4 Rpt/Process Not functioning - workaround avail		Cobol License	2016/01/25 10:55:54		2016/01/26
INC1868286	Closed	2 Essential Process Halted		MCFU92 environment is very slow	2016/01/26 14:36:57		2016/01/27
INC1868611	Closed	2 Essential Process Halted		unable to extend temp segment by 16 in tablespace PSTEMP	2016/01/26 18:43:34		2016/01/27
INC1869815	Closed	4 Rpt/Process Not functioning - workaround avail		Attachment Server is not configured	2016/01/27 16:48:49		2016/01/28
INC1869835	Closed	3 Rpt/Process Not functioning - workaround NOT avail		Access to production Database	2016/01/27 17:02:44		2016/01/28
INC1870663	Closed	2 Essential Process Halted		Excel to CI upload not working in Production	2016/01/28 11:28:44		2016/01/28

Performance and Capacity Metrics

Metrics have been analyzed for the following systems:

- PeopleSoft application and web servers (Availability, CPU, RAM and Network)
- Firewall CPU and Inside interface.

Report Data	
Reporting Period	2016-1-20 00:00:00 to 2016-1-27 00:00:00
System Name	
System Description	Primary PeopleSoft Financials Application Server

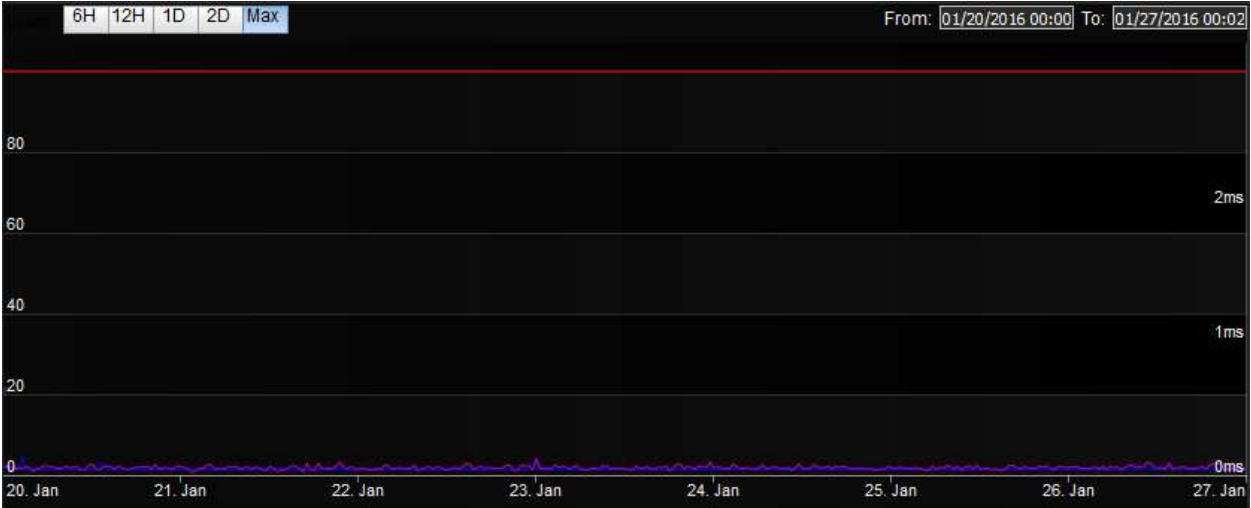


	Chart Data - System Vitals			
	Current Week		Previous Week	
Availability	Avail = 100 %		Avail = %	
CPU Utilized	Max = 11 %	Avg= 1 %	Max = %	Avg= %
Memory (RAM) Utilized	Max = 7 %	Avg = 2 %	Max = %	Avg = %

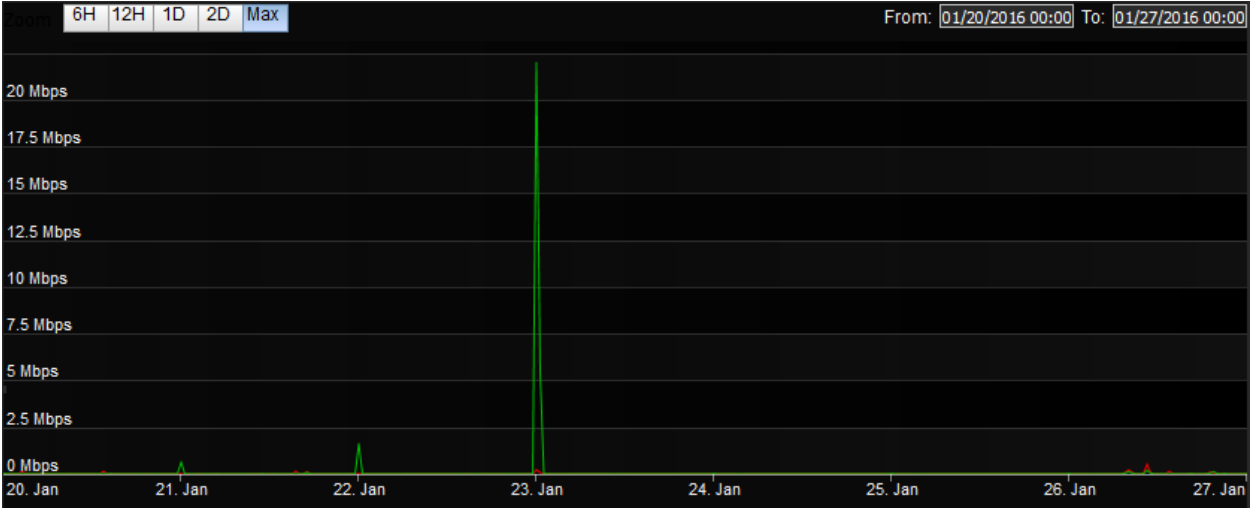


	Chart Data Network Interface (eth0)			
	Current Week		Previous Week	
Inbound Traffic (Mbps)	Max =0.8 Mbps	Avg = 0.01	Max = Mbps	Avg = Mbps

	Chart Data Network Interface (eth0)			
	Current Week		Previous Week	
		Mbps		
Outbound Traffic (Mbps)	Max=44.0 Mbps	Avg = 0.09 Mbps	Max= Mbps	Avg = Mbps

Reporting Period	2016-1-20 00:00:00 to 2016-1-27 00:00:00
System Name	
System Description	Secondary PeopleSoft Financials Application Server



	Chart Data - System Vitals			
	Current Week		Previous Week	
Availability	Avail = 100 %		Avail = %	
CPU Utilized	Max = 9.8 %	Avg= 0.9 %	Max = %	Avg= %
Memory (RAM) Utilized	Max = 8 %	Avg = 2 %	Max = %	Avg = %

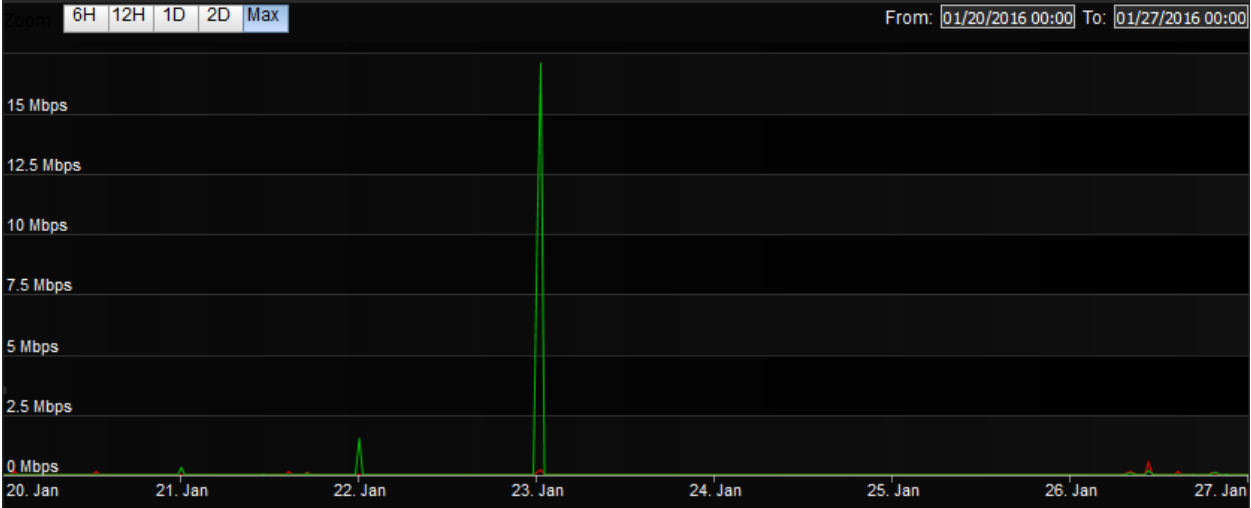


	Chart Data Network Interface (eth0)			
	Current Week		Previous Week	
Inbound Traffic (Mbps)	Max = 0.8 Mbps	Avg = 0.01	Max = Mbps	Avg = Mbps



		Mbps		
Outbound Traffic Mbps)	Max= 34.2 Mbps	Avg = 0.09 Mbps	Max= Mbps	Avg = Mbps

Reporting Period	2016-1-20 00:00:00 to 2016-1-27 00:00:00
System Name	
System Description	Primary PeopleSoft Financials Web Server



	Chart Data - System Vitals			
	Current Week		Previous Week	
Availability	Avail = 100 %		Avail = %	
CPU Utilized	Max = 13 %	Avg= 3 %	Max = %	Avg= %
Memory (RAM) Utilized	Max = 22 %	Avg = 11 %	Max = %	Avg = %

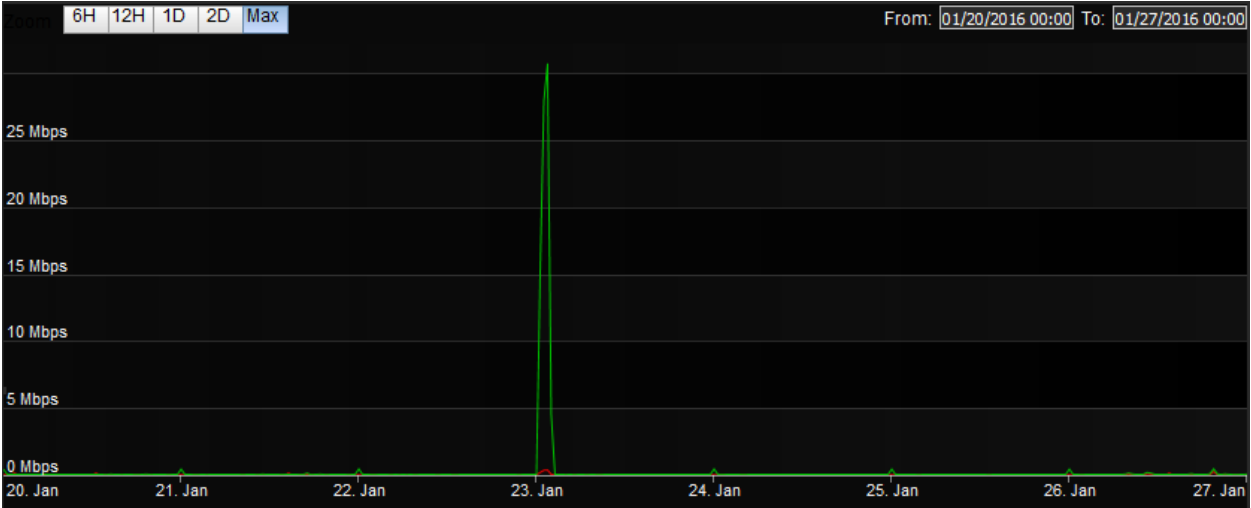


	Chart Data - Network Interface (eth0)			
	Current Week		Previous Week	
Inbound Traffic (Mbps)	Max = 0.39 Mbps	Avg = 0.01 Mbps	Max = Mbps	Avg = Mbps
Outbound Traffic	Max=33.4 Mbps	Avg = 0.3 Mbps	Max= Mbps	Avg = Mbps

Mbps)				
Reporting Period	2016-1-20 00:00:00 to 2016-1-27 00:00:00			
System Name				
System Description	Secondary PeopleSoft Financials Web Server			

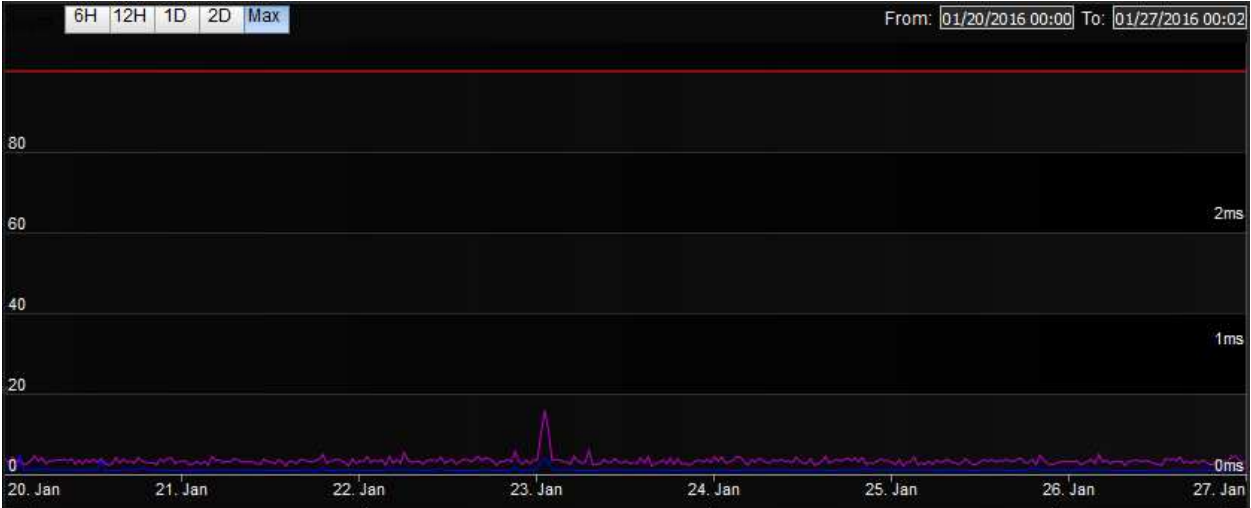


	Chart Data - System Vitals			
	Current Week		Previous Week	
Availability	Avail = 100 %		Avail = %	
CPU Utilized	Max = 11.0 %	Avg= 1.08 %	Max = %	Avg= %
Memory (RAM) Utilized	Max = 18 %	Avg = 3 %	Max = %	Avg = %

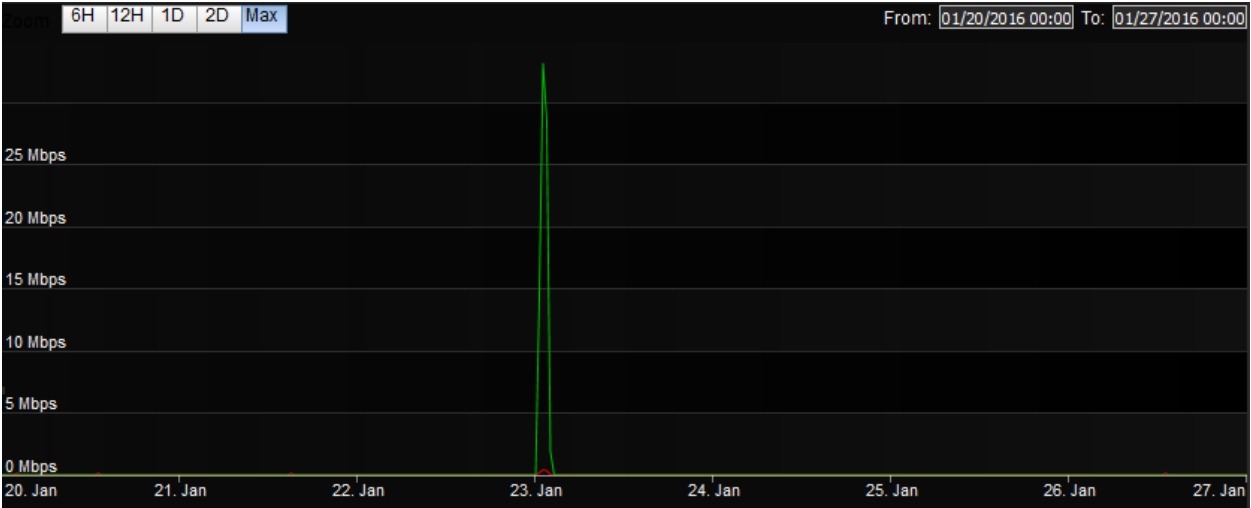


	Chart Data - Network Interface (eth0)			
	Current Week		Previous Week	
Inbound Traffic (Mbps)	Max = 0.46 Mbps	Avg = 0.01 Mbps	Max = Mbps	Avg = Mbps
Outbound Traffic (Mbps)	Max= 36 Mbps	Avg = 0.23 Mbps	Max= Mbps	Avg = Mbps

Reporting Period	2016-1-20 00:00:00 to 2016-1-27 00:00:00
System Name	NJ-MCH-DB1
System Description	Primary PeopleSoft Database Server

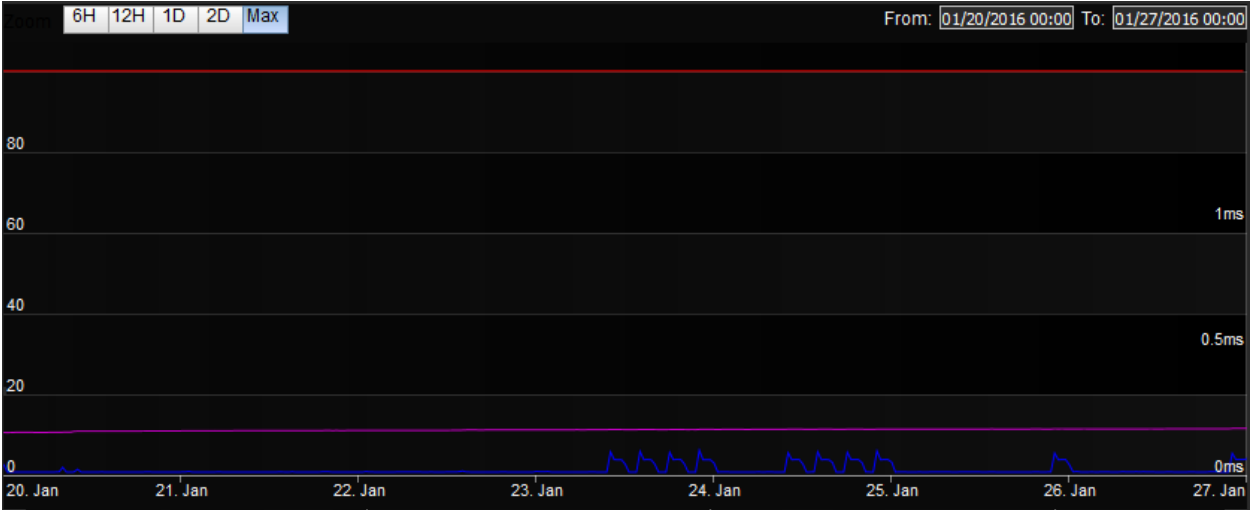


	Chart Data –System Vitals			
	Current Week		Previous Week	
Availability	Avail = 100 %		Avail = %	
CPU Utilized	Max = 7.3 %	Avg= 1.26 %	Max = %	Avg= %
Memory (RAM) Utilized	Max = 12 %	Avg = 11 %	Max = %	Avg = %

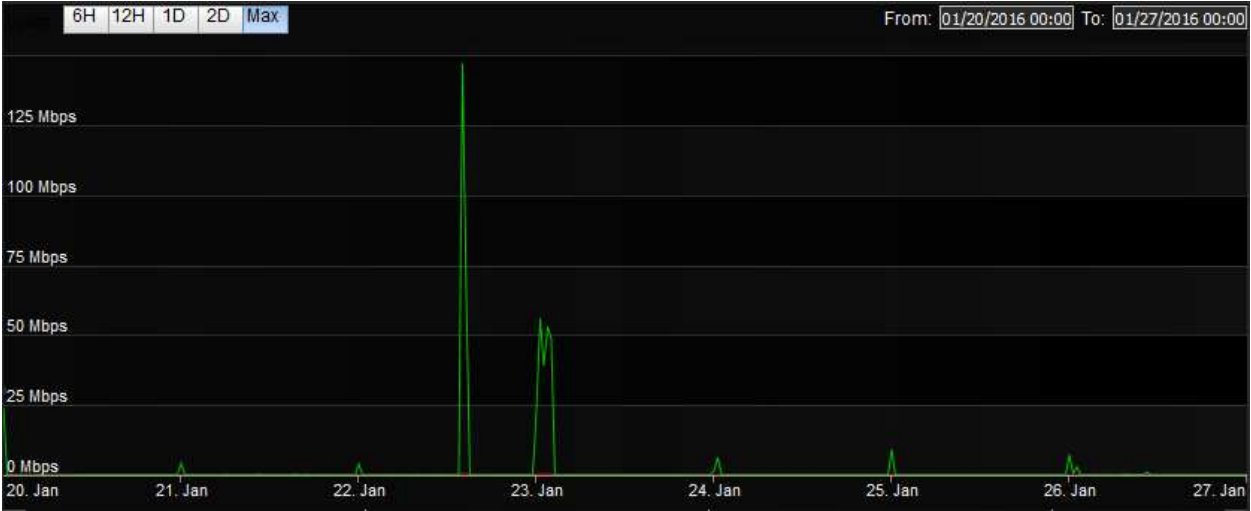


	Chart Data - Network Interface (Bond0)			
	Current Week		Previous Week	
Inbound Traffic (Mbps)	Max = 0.98 Mbps	Avg = 0.04 Mbps	Max = Mbps	Avg = Mbps
Outbound Traffic (Mbps)	Max=158.7 Mbps	Avg = 1.51 Mbps	Max= Mbps	Avg = Mbps

Reporting Period	2016-1-20 00:00:00 to 2016-1-27 00:00:00
System Name	
System Description	Secondary PeopleSoft Database Server

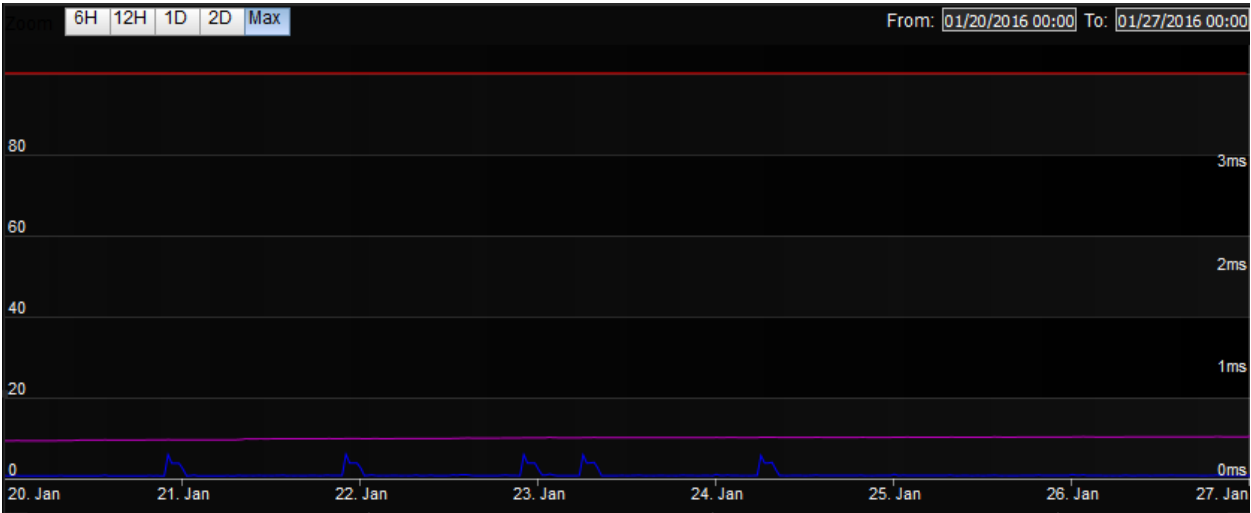


	Chart Data –System Vitals			
	Current Week		Previous Week	
Availability	Avail = 100 %		Avail = 100 %	
CPU Utilized	Max = 7.07 %	Avg= 0.97 %	Max = %	Avg= %
Memory (RAM) Utilized	Max = 11 %	Avg = 10 %	Max = %	Avg = %

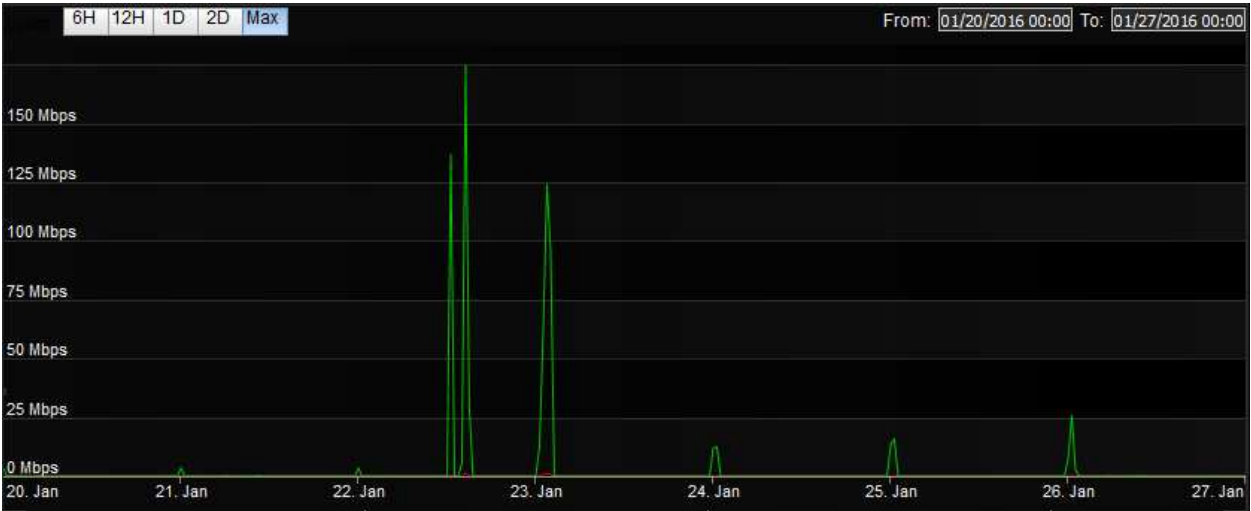


	Chart Data - Network Interface (Bond0)			
	Current Week		Previous Week	
Inbound Traffic (Mbps)	Max = 1.37 Mbps	Avg = 0.03 Mbps	Max = Mbps	Avg = Mbps
Outbound Traffic (Mbps)	Max=191.2 Mbps	Avg = 2.23 Mbps	Max= Mbps	Avg = Mbps



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

CherryRoad can provide historical, statistical and usage reports that can be printed and viewed locally. In the near future, those reports will be available on the client portal.

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

CherryRoad on demand deployment is supported 24x365.

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

CherryRoad's customer self-service portal is available 24x7x365 in addition to our service desk to support client requirements.



### 8.13 (E) Cloud Security Alliance Questionnaires

*Describe your level of disclosure with CSA Star Registry for each Solution offered.*

*a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3.*

CherryRoad has completed Level-1 of the CSA STAR Registry Self-Assessment with a goal of Level -2 certification completed by EOY 2016.

*b. Completion of Exhibits 1 and 2 to Attachment B.*

Please see:

- **Technical Response – 8.13 b – CherryRoad Exhibit 1.xls.**

*c. Completion of a CSA STAR Attestation, Certification, or Assessment.*

CherryRoad will complete this certification by the end of 2016.

*d. Completion CSA STAR Continuous Monitoring.*

CherryRoad will complete this certification by the end of 2016.



## 8.14 (E) Service Provisioning

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

CherryRoad's client self-provisioning portal provides the purchasing agent with the flexibility to build servers on demand. In the event of an emergency, change handling CherryRoad change control board will review and schedule changes based on urgency, impact, and risk.

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

CherryRoad solution provisioning occurs over two phases. The first is the initial onboarding and setup. Typically, this can be completed in 30-60 days from engagement start. This includes defining user access and providing initial on-boarding requirements. In the second phase or steady state, most provisioning is completed within hours via automation via the client self-service portal.



## 8.15 (E) Back Up And Disaster Plan

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

CherryRoad has the ability to provide an additional retention service and retain data by entity for as long as necessary.

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

CherryRoad maintains two geographically diverse data centers with fully redundant infrastructures. Typically, inherent disaster recovery risks occur at the application or licensing layer where certain applications are not well suited for real time replication and recovery. CherryRoad mitigates this by utilizing our expertise to work with our clients to provide solutions for these situations.

*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.*

CherryRoad uses best of breed hardware and software to ensure that data is protected in the case of a data center loss. This includes the use of SAN replication and EMC RecoverPoint, backup to EMC DataDomain appliance, use of F5 load balancers, Oracle Exadata and Exalogic Engineered systems and VMware Site Recovery Manager. CherryRoad also ensures that each data center has enough capacity in the case of a full site failure.





## 8.16 (E) Solution Administration

### 8.16.1 Ability of the Purchasing Entity to fully manage identity and user accounts.

CherryRoad can supply or integrate into most environments. This includes Active Directory or other LDAP solutions.

### 8.16.2 Ability to provide anti-virus protection, for data stores.

CherryRoad includes antivirus protection as part of the standard virtual system build.

### 8.16.3 Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider.

All Purchasing Entity data stored within the PaaS and IaaS platforms can be provided to a successor solution provider. In the case of IaaS virtual machine files will be provided. For PaaS DB files and DB logs will be provided.

### 8.16.4 Ability to administer the solution in a distributed manner to different participating entities.

CherryRoad can provide the ability to administer the solution to any number of individuals at any number of locations.

### 8.16.5 Ability to apply participating entity defined administration policies in managing solution

Administration policies can be fully customized and managed by the State.



## 8.17 (E) Hosting and Provisioning

### 8.17.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Provisioning and automation provides the ability to allocate the various CherryRoad PaaS and IaaS resources from the physical environment necessary to support the implementation of database services that support agreed upon operational and performance characteristics through an automated process.

The following capabilities define the DBaaS Service Deployment:

- Database Client Interface – Provides the Consumer with network access to their database resources through native database protocols. Database Client Interface provides logical isolation to the database instance through authentication and authorization services.
- Database Resources – Database Resources represents the collection of capabilities required by the instantiated database instance through logical and physical compute, storage, and network services in order to run / operate the database software within the configuration defined by the service offering.
- Database Configuration – The Database Configuration represents the definition of what database characteristics and resources are allocated for the implementation of the instantiated database within a given shared service deployment model. The database configuration supports the ability of the database instance to be implemented within the different shared resource models, while allowing for appropriate segmentation and isolation from other database service consumer instances.
- Database Deployment – The Database Deployment capabilities provides for the implementation of the database instance through different implementation models supporting various service level definitions and resource segmentation approaches. These capabilities allow for the database to be deployed into different resource configurations which allows for sharing of different categories of resources that may be tuned for specific database workloads, security, and availability characteristics.
- Database Resource Segmentation – The Database Resource Segmentation capabilities allows for the operations of the database instance within a shared resource pool in a manner such that the Consumers are unaware of their participation in a multi-tenancy deployment. Database Resource Segmentation is applied through various techniques depending upon the resources to be shared, what type of isolation is required, and the deployment model to which it is applied.
- Database Resource Metrics – The resource metrics capabilities provides the IT organization with the ability to monitor and affect operational change based upon the utilization of logical and physical resources for each database instance within the shared service environment. The metrics required must support the ability to capture the utilization of resources by the individual database instances as well as the performance of the aggregated resources used to support the shared database environment. The specific metrics required will be determined by the methods in which resource utilization is charged-back to the Consumer as defined through the service offerings defined within the organizations service catalog.



## 8.18 (E) Trial and Testing Periods (Pre- and Post-Purchase)

*8.18.1 Describe your testing and training periods that your offer for your service offerings.*

CherryRoad provides both transitional and steady-state training and testing. Training will be provided for both the IAAS and PAAS service offerings. Training will focus on our clients' ability to access and request services through the CherryRoad Service/Help desk. Specifically training will be provided on how to request a service, track a service request and engage the CherryRoad Help Desk for question and answers and the mechanics of how to use our services. Training schedule will be determined through the transition and be provided quarterly once in steady-state. In regards to Testing, all clients will be required to perform some level of acceptance testing whenever CherryRoad is required to perform upgrade/updates on an individual technical stack which may impact client services. Testing schedules and releases to production would be approved by both the client and CherryRoad before any final schedules are determined.

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

CherryRoad will provide an internal demo system for proof of concept for evaluation that verifies our ability to meet mandatory requirements.

*8.18.3 Offeror must describe what training and support it provides at no additional cost.*

Training will be provided to ensure each client understands how to access their respective system and request services. Additionally, targeted training (i.e. application, etc) can be provided at an additional cost – see rate card.



## 8.19 (E) Integration and Customization

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

CherryRoad PaaS and IaaS solutions accommodate most OS platforms, Windows, Linux, or Unix.

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

CherryRoad can provide custom templates to address each purchasing agents requirements. Once complete, these custom templates can be accessed and provisioned via the self-service portal.



## 8.20 (E) Marketing Plan

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

CherryRoad will market our cloud services through Public Sector industry specific conferences and events for state/local government, higher education, and K-12 education, as well as NASPO sponsored conference on “How to Market to State Governments.”

In addition to industry specific events, we will conduct social media, email campaigns, webinars, and issue press releases.



## 8.21 (E) Related Value-Added Services to Cloud Solutions

*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.*

### Single Sign On, Secure Access and Authentication Platform

Service provides customer gateway into the cloud giving clients one entrance into their systems. back and forth authentication is seamless to end user

- Multi-factor authentication provides a secure path with strong access controls.
- Flexibility to integrate with client directories (i.e. active directory), protocols and tools.
- One secure portal within the CherryRoad Cloud.
- Streamlined access to applications with one set of credentials (Single Sign-On).
- Users can login from anywhere with any device.



## 8.22 (E) Supporting Infrastructure

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

CherryRoad cloud managed service offerings may require purchasing entity to provide network services required to support the requested PaaS and IaaS services. In some cases any additional technical requirements that may be required to fulfill the service procurement process.

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

CherryRoad will be responsible for the installation and procurement of additional infrastructure to support purchasing agents' server and DB requirements outside of purchasing agents network connectivity.



## 8.23 (E) Alignment of Cloud Computing Reference Architecture

*Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).*

Cherry Road cloud architecture is directly derived and based on the NIST Cloud Computing Reference Architecture specifically for PaaS and IaaS service domains