Contract #: AR3099

STATE OF UTAH COOPERATIVE CONTRACT

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

Ensono, LP
Name

3333 Finley Rd Downers
Street Address

Grove	IL	60515
City	*State*	*Zip*

Vendor # VC226530 Commodity Code #: 920-05 Legal Status of Contractor: Partnership

Contact *Name:* Doris Gaiser *Phone Number:* 501-952-4757 *Email:* doris.gaiser@ensono.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

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

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

5. CONTRACT PERIOD: Effective Date: Thursday, May 23, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

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

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

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

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

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

Douglas Borgmann
Douglas Borgmann (May 28, 2019)

May 28, 2019

Contractor's signature — Date

Douglas Borgmann — Deputy General Counsel

Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes
Christopher Hughes (May 28, 2019)

May 28, 2019

Director, Division of Purchasing — Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

Cause means the failure of a party to perform a material obligation under this Master Agreement or a Participating Addendum, which failure is not remedied within thirty (30) days following receipt of written notice.

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

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees,

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

subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

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

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

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

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

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

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

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The

consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

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

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

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

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

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

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

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

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

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

into a Participating Addendum.

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

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

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

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

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

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

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

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

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

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

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

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

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

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

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State, except that Contractor may assign or subcontract its rights and obligations under this Master Agreement or any Participating Addendum in whole or in part, to any affiliate or successor in interest, provided it gives the Lead State and the applicable Purchasing Entity notice of such assignment. In either case written notice shall be provided 30 days prior to the proposed assignment action.

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly

known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information. Contractor will not be deemed to have accessed, received, or be in the possession of Confidential Information solely by virtue of the fact that the Lead State or the applicable Purchasing Entity transmits, receives, accesses or stores such information through its use of Contractor's services.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

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

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

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

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

(1) Nonperformance of contractual requirements; or

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

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

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

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

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification and Limitation of Liability

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

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property

rights ("Intellectual Property Claim") of another person or entity.

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

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

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

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

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

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

THIS SECTION 13.B. STATES THE ENTIRE OBLIGATION OF CONTRACTOR AND ITS SUPPLIERS, AND THE EXCLUSIVE REMEDY OF THE INDEMNIFIED PARTIES, IN RESPECT OF ANY INFRINGEMENT OR ALLEGED INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR PROPRIETARY RIGHTS. THIS INDEMNITY OBLIGATION AND REMEDY ARE GIVEN TO THE INDEMNIFIED PARTIES SOLELY FOR THEIR BENEFIT AND IN LIEU OF, AND CONTRACTOR DISCLAIMS ALL WARRANTIES, CONDITIONS, AND OTHER TERMS OF NON-INFRINGEMENT WITH RESPECT TO ANY PRODUCT.

c. Limitation of Liability. (1) NO PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, RELIANCE, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR ANY LOST OR IMPUTED PROFITS OR REVENUES, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH LIABILITY IS ASSERTED, AND REGARDLESS OF WHETHER A PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITY.

(2) EXCEPT FOR LIABILITY ARISING FROM CONTRACTOR'S INDEMNIFICATION OBLIGATIONS IN SECTION 13(b) ABOVE AND THE LEAD STATE OR ANY PARTICIPATING ENTITY'S OBLIGATION TO PAY ALL FEES UNDER THIS AGREEMENT, CONTRACTOR'S TOTAL AGGREGATE LIABILITY ARISING FROM OR RELATED TO THIS MASTER AGREEMENT SHALL IN NO EVENT EXCEED DIRECT DAMAGES IN AN AMOUNT EQUAL TO THE GREATER OF (i) TWELVE (12) TIMES THE MONTHLY RECURRING CHARGES PAID OR PAYABLE UNDER THE APPLICABLE PARTICIPATING ADDENDUM IN THE MONTH IMMEDIATELY PRECEDING THE DATE OF THE CLAIM OR (ii) THREE MILLION DOLLARS ($3,000,000).

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 a claim basis. The minimum acceptable limits shall be as indicated below, with Ensono also responsible for any related deductible, for each of

the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

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

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

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

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, and (2) 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, and endorsements). Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

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

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

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

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

19. Ordering

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

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

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing

procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

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

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

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

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

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

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any

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

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

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

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

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

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

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

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

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

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

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

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

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

or more stringent than those specified in the Solicitation.

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

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

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

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

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

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

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

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

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

30. Data Privacy: The parties will comply in all material respects with all laws related to data privacy and security applicable to the provision (in the case of Contractor) and use (in the case of each Participating Entity) of the Services provided to each Participating Entity, including IRS Pub 1075. Each Purchasing Entity is responsible for selecting and using the level of security protection needed for its data stored or transmitted via the Services and using reasonable information security practices, including those relating to the encryption of data. 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 are true and accurate in all material respects.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.

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

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

32. Transition Assistance:

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

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

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

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

Purchase Order.

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

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

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

37. Governing Law and Venue

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

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

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely

and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

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

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

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

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

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

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities,

other than payment, are required under the Master Agreement.

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

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

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

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

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

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

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

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

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

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

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

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

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

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

subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

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

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

Exhibit 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 from a Purchasing Entity in the performance of the Master Agreement shall become and remain the property of such 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 such 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 promptly 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, to the extent a Data Breach is a direct result of Contractor's breach of its contractual obligations to encrypt Personal Data or otherwise prevent its release in the Master Agreement, and subject to the terms set forth therein, 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 Addendum 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 reasonable and lawful discretion, as a result of the background or criminal history investigation, the Purchasing Entity shall have the right to request prompt replacement of the person and if Ensono does not promptly replace such person, the Purchasing Entity may terminate the Participating Addendum and any related service agreement by delivering Ensono written notice.

9. Access to Security Logs and Reports:

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

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

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

discretion and at the Purchasing Entity's expense, subject to the terms set forth in the Master Agreement.

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 are reasonably likely to materially and adversely affect 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 other similarly-situated users at no additional costs.

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 except as otherwise expressly stated in the Participating Addendum.

Contractor will exercise commercially reasonable efforts to 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 reasonably 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 unreasonable 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 providing a material portion of the Services under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

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

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

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

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Infrastructure as a Service (IaaS)

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	See Below

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)

In addition to (meaning, as a stand-alone service offering), or in connection with, the foregoing, Contractor may provide (and the Scope of Services shall be deemed to include) other available value-added Services as described in Contractor's response to the Solicitation including, without limitation, Mainframe or Distributed Systems -related service offerings, professional services, consulting and advisory services and security-enabling services.

Attachment C - Pricing Discounts and Schedule

Contractor: Ensono, LP

Pricing Notes

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

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

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

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

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

Cloud Service Model: Infrastructure as a Service (IaaS)

IaaS Minimum Discount % Off

Description	Discount
IaaS Minimum Discount %*	5.00%

*applies to all OEM's offered within the IaaS service model

Additional Value Added Services

Item Description	Onsite Hourly Rate NVP Price	Onsite Hourly Rate Catalog Price	Remote Hourly Rate NVP Price	Remote Hourly Rate Catalog Price
Maintenance Services	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card
Professional Services				
Deployment Services	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card
Integration Services	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card
Consulting/Advisory Services	240.00	300.00	200.00	250.00
Architectural Design Services	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card
Statement of Work Services	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card
Partner Services	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card
Training Deployment Services	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card	See IaaS Rate Card
Security Engineer - Standard	216.00	268.80	180.00	224.00
Security Engineer - Expert	288.00	357.60	240.00	298.00
Project Manager	258.00	324.00	215.00	270.00
Systems Administrator	204.00	246.00	170.00	205.00
Database Administrator	240.00	300.00	200.00	250.00
Network Engineer	288.00	357.60	240.00	298.00
Infrastructure Architect	288.00	357.60	240.00	298.00

Ensono FLEX Offerings:	Deliverable Rates NVP Price	Deliverable Rates Catalog Price
Managed Azure – Platform/Core Service Management	25% of Consumed Azure Revenue	30% of Consumed Azure Revenue
Managed Azure – Managed IaaS/VMs	25% of Consumed Azure Revenue	30% of Consumed Azure Revenue
Managed IBM i Server (See Note 1 below)	$10,910/Month	$11,485/Month
Managed Server (See Note 2 below)	$310/Month	$327/Month
Managed z/OS > 250 MIPS (See Note 3 below)	$703/MIP/Month	$740/MIP/Month
Managed z/OS > 500 MIPS (See Note 3 below)	$570/MIP/Month	$600/MIP/Month
Managed z/OS > 1,500 MIPS (See Note 3 below)	$390/MIP/Month	$410/MIP/Month

Attachment C - Pricing Discounts and Schedule

Contractor: Ensono, LP

Note 1: Managed IBM I Server price includes (1) LPAR Fully Managed Premium Service with Replication; 1 CPU, 1 TB disk, 2 TB Tape, Firewall/Switches, 50 Mbps VPN, IBM I operating system.

Minimum term of 36 months. Migration fees are not included in this price.

Note 2: Managed Server price includes (4) virtual CPU, 10 GB RAM, 150 GB standard performance storage, Windows or Linux operating system management.

Minimum term of 36 months. Migration fees are not included in this price.

Note 3: Managed z/OS price includes:

250 MIPS, 10 TB DASD, 100 TB Virtual Tape; z/OS, CICS, DB2, Cobol; CA software; Ensono tools; 1 LPAR, 2 CICS Regions, 1 DB2 instance; technical managed services.

500 MIPS, 20 TB DASD, 200 TB Virtual Tape; z/OS, CICS, DB2, Cobol; CA software; Ensono tools; 1 LPAR, 4 CICS Regions, 2 DB2 instances; technical managed services.

1,500 MIPS, 60 TB DASD, 600 TB Virtual Tape; z/OS, CICS, DB2, Cobol; CA software; Ensono tools; 3 LPARs, 12 CICS Regions, 6 DB2 instances; technical managed services.

Minimum term of 36 months. Migration fees, replication, and job scheduling are not included in this price.

Ensono Managed AWS Services Rate Card

Monthly Management Fees	Billing Unit	List Price	Percentage Savings	NASPO Rate
Option A: AWS Premium Management (24x7x365 with 15-Minute Response Time) - Spend Greater than $20,000 per month	AWS Premium Management	40%	5.00%	35%
Option B: AWS Premium Management (24x7x365 with 15-Minute Response Time) - Spend Less than $20,000 per month (minimum applies)	AWS Premium Management - Minimum	$ 5,000.00	5.00%	$ 4,750.00
Option C: AWS Managed Essentials (9x5 Central Time Zone Support with 24-Hour Response Time) - Spend Greater than $20,000 per month	AWS Managed Essentials	30%	5.00%	25%
Option D: AWS Managed Essentials (9x5 Central Time Zone Support with 24-Hour Response Time) - Spend Less than $20,000 per month (minimum applies)	AWS Managed Essentials - Minimum	$ 3,000.00	5.00%	$ 2,850.00
AWS Business Support - Required for All Managed Clients	AWS Business Support	12%	5.00%	7%

Deployment/Installation Fees	Billing Unit	List Price	Percentage Savings	NASPO Rate
Create new AWS account, setup IAM, billing, monitoring, automation, etc.	AWS Account Setup	$ 1,730.00	5.00%	$ 1,643.50
Create new auto-scale group and settings, monitoring, automation	AWS Auto-Scale Group	$ 265.00	5.00%	$ 251.75
Create new AMI for AWS and RHEL Linux instance and put in infrastructure as code repository	AWS Linux instance	$ 380.00	5.00%	$ 361.00
Create new AMI for Windows instance and put in infrastructure as code repository	AWS Windows instance	$ 380.00	5.00%	$ 361.00
Create new RDS instance in a single availability zone and put in infrastructure as code repository	AWS RDS single availability zone	$ 200.00	5.00%	$ 190.00
Create new RDS instance in HA configuration across multiple availability zones and put in infrastructure as code repository	AWS RDS Multi-Availability Zone	$ 200.00	5.00%	$ 190.00
Create a new backup policy and put in infrastructure as code repository	Backup Policy	$ 160.00	5.00%	$ 152.00
Create a client specific monitoring dashboard	Custom Monitoring Dashboard	$ 495.00	5.00%	$ 470.25
Create new ELB/ALB without SSL certificate and put in infrastructure as code repository	AWS ELB/ALB no-SSL	$ 135.00	5.00%	$ 128.25
Create new ELB/ALB with SSL certificate and put in infrastructure as code repository	AWS ELB/ALB with SSL	$ 265.00	5.00%	$ 251.75
Create new Security Group and put in infrastructure as code repository	AWS Security Group	$ 135.00	5.00%	$ 128.25
Create up to 5 S3 buckets and put in infrastructure as code repository	AWS S3 upto 5 Buckets	$ 135.00	5.00%	$ 128.25

Attachment C - Pricing Discounts and Schedule

Contractor: Ensono, LP

Create new Route53 domain and put in infrastructure as code repository	AWS Route53 Domain (<15 records)	$ 27.00	5.00%	$ 25.65
Create new Elasticache instance in a single availability zone and put in infrastructure as code repository	AWS Elasticache single availability zone	$ 235.00	5.00%	$ 223.25
Create new Elasticache instance in multiple availability zones and put in infrastructure repository	AWS Elasticache multiple availability zone	$ 235.00	5.00%	$ 223.25
Create new VPC and put in infrastructure as code repository	AWS VPC Standard	$ 135.00	5.00%	$ 128.25
Create new VPN connection and put in infrastructure as code repository	AWS VPN	$ 70.00	5.00%	$ 66.50
Create new NAT Gateway and put in infrastructure as code repository	AWS NAT Gateway	$ 70.00	5.00%	$ 66.50
AWS Engineering and Operations	Hour	$ 225.00	5.00%	$ 213.75

ENSONO TECHNICAL RESPONSE

8 TECHNICAL REQUIREMENTS

If applicable to an Offeror's Solution, an Offeror must provide a point by point response to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

8.1(M)(E) TECHNICAL REQUIREMENTS

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

Ensono provides Managed AWS Infrastructure using AWS' NIST compliant cloud infrastructure services.

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

Ensono is in full compliance with Attachments C & D outlined in this RFP.

8.1.3As 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.

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete client privacy and segregation. AWS's highly secure data centers use:

- State-of-the-art electronic surveillance
- Multi-factor access control systems
- Maintenance of strict, least-privileged-based access authorizations

In addition, Ensono utilizes AWS' environmental systems that are designed to minimize the impact of disruptions to operations. Multiple geographic regions and availability zones allow clients to remain resilient in the face of most failure modes, including natural

© 2018 Ensono, LP. All rights reserved.

disasters or system failures. AWS manages over 1,800 security controls to provide an optimally secure environment for all of its clients.

Furthermore, network traffic between AWS regions, Availability Zones, and individual data centers travels over private network segments by default. These private network segments are fully isolated from the public internet, and not routable externally. AWS resources can be configured to reside only on isolated AWS network segments, and to avoid using any public IP addresses or routing over the public internet.

In addition to a strong security posture and isolation, AWS offers further Isolation and controls by leveraging GovCloud, which is an ideal fit for "high impact data." Specifically, GovCloud, is an isolated region in an environment where clients can run ITAR-compliant applications with special endpoints that use only Federal Information Processing Standard (FIPS) 140-2 encryption.

It is important that clients understand some important basics regarding data ownership and management in the cloud-shared responsibility model:

1. Clients continue to own their data.
2. Clients choose the geographic location(s) in which to store their data—it does not move unless the client decides to move it.
3. Clients can download or delete their data whenever they like.
4. Clients should consider the sensitivity of their data, and decide if and how to encrypt the data while it is in transit and at rest.

AWS provides clients with the ability to delete their data. However, AWS clients retain control and ownership of their data. It is the client's responsibility to manage their data.

NIST Characteristic – On-Demand Self Service: Amazon Web Services, Inc. (AWS) provides clients of all sizes with on-demand access to a wide range of cloud infrastructure services, charging you only for the resources you actually use. AWS enables you to eliminate the need for costly hardware and the administrative pain that goes along with owning and operating it. Instead of the weeks and months it takes to plan, budget, procure, set up, deploy, operate, and hire for a new project, our clients can simply sign up for AWS and immediately begin deployment in the cloud with the equivalent of 1, 10, 100, or 1,000 servers. Whether an organization needs to prototype an application or host a production solution, AWS makes it simple for clients to get started and be productive.

NIST Characteristic – Broad Network Access: AWS provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. Cloud computing providers such as AWS own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application, mobile client, or programmatically through published and well-documented APIs.

© 2018 Ensono, LP. All rights reserved.

NIST Characteristic – Resource Pooling: The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each client from other clients. AWS systems are designed to prevent clients from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in October 2010.

NIST Characteristic – Rapid Elasticity: AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications, scale up as your workload grows, and scale down based on demand. Clients need to be confident that their existing infrastructure can handle a spike in traffic and that the spike will not interfere with normal business operations. Elastic Load Balancing and Auto Scaling can automatically and instantly scale a client's AWS resources up to meet unexpected demand, and scale those resources down just as fast if demand decreases.

NIST Characteristic – Measured Service: AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

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.

Ensono offers Managed AWS Services on top of the AWS IaaS solution. We do not use subcontractors to fulfill this service. We have fully certified AWS expertise around compute, storage, and networking.

Additionally, Ensono provides a full, private cloud offering using VMWare SDDC. Ensono performs the 1st and 2nd level triage of incidents through to 3rd level resolution. Advanced monitoring is included to help proactively reduce Incidents before they happen

© 2018 Ensono, LP. All rights reserved.

and reduce Incident resolution time when Incidents do happen. The Ensono Cloud Service is multi-tenant with specific services being single tenant.

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.

Ensono does not intend to leverage subcontractors to deliver any of the defined services. We may, on a case-by-case basis, leverage subcontractors for specific work that would be identified and agreed-to by the client.

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

Not applicable

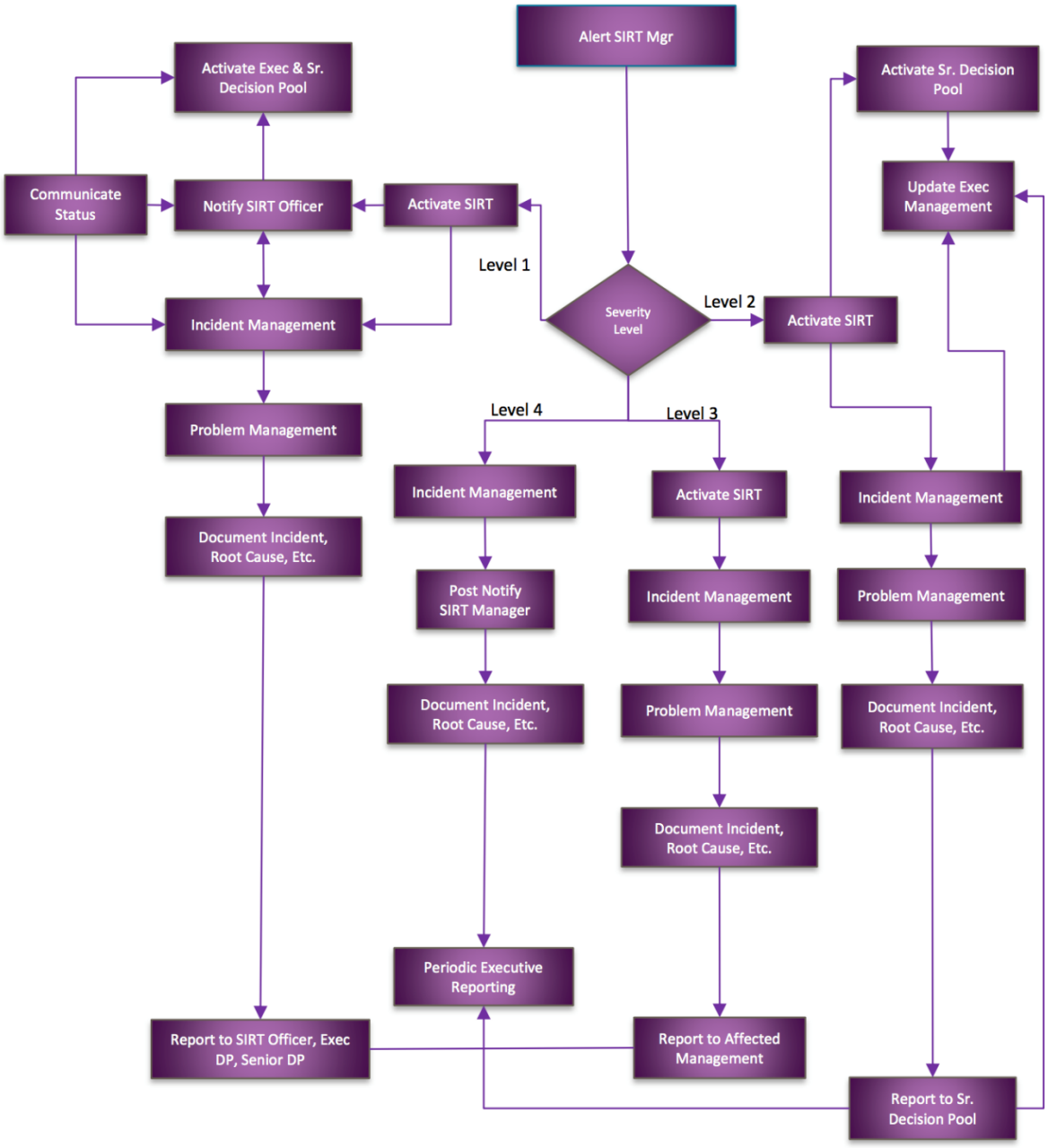
8.3(E) WORKING WITH PURCHASING ENTITIES

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.**

For suspected incidents or Data Breaches, Ensono follows our Security Incident Response Plan, which is driven by Ensono's Security Operations Center (SOC). The response times, methodology, and methods of communication are further explained in the document **Ensono Addendum-SecurityIncidentResponsePlan.PDF**. The following flow chart also illustrates our Security Incident Response Plan.

© 2018 Ensono, LP. All rights reserved.



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.

Ensono does not use or market client's data, nor does it permit the pushing of agents, adware, etc. into a client's environment under any circumstances.

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

© 2018 Ensono, LP. All rights reserved.

Ensono works with all of our clients to create an isolated user-test/staging/QA environment with appropriate security controls, network isolation, and network segmentation.

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

All of Ensono's services, web portals, and websites comply with the Americans with Disability Act.

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

Ensono's and AWS' content can be delivered through all modern browsers, including Internet Explorer, Firefox, Chrome, and Safari.

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.

Ensono will meet with the Purchasing Entity, cooperate and hold a meeting to determine storage of sensitive or personal information and related compliance requirements. Additionally, we use a standard design process and architectural engagement process with appropriate controls in place to identify environment(s) with personal and/or sensitive information.

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.

Timelines will vary on a case-by-case basis, depending on the size of the engagement. Typical engagements will last between 60-90 days to get a client onboarded with all of the appropriate controls, environments, and security instantiated.

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

- How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.
    - Ensono will maintain governance around what new products are released and ensure that they adhere to the standards outlined with section 2.12.
- How Offeror will maintain discounts at the levels set forth in the contract.

© 2018 Ensono, LP. All rights reserved.

  - Ensono will continue to maintain the discount levels set forth in the contract for the remainder of the contract. We do forward pricing savings, including discounts, to ensure that we will be able to pass on savings to our clients throughout the life of the contract.
- How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.
  - Ensono's Program Management Office will setup a structure for governing notifications of changes and manage via a change management process.
- How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.
  - Ensono's Client Service Organization (CSO) will communicate, verbally and in writing, any changes, positive or negative, to the respective Purchasing Entities.

8.4(E) CUSTOMER SERVICE

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

- Quality assurance measures;
  - Ensono's Client Service Organization (CSO) is measured specifically by Net Promoter Scores (NPS) and centered around quality controls and quality assurance for our client's and Purchasing Entities.
- Escalation plan for addressing problems and/or complaints; and
  - Ensono's Client Service Organization (CSO) has a defined process for escalation of problems/issues/complaints:

© 2018 Ensono, LP. All rights reserved.

Assignment Escalations	Closure Escalations	Elevate / Notify
For Priority 1 and 2, escalations start after ticket is opened for 15 minutes until ticket is moved to assigned status. For Priority 3 and 4, escalations start when ticket is within 1 hour of service level agreement being missed.	Standard service timeframe is within 1 hour of being missed.	Assignee
For Priority 1 and 2, escalations start after ticket is opened for 15 minutes until ticket is moved to assigned status. For Priority 3 and 4, escalations start when ticket is within 45 minutes of service level agreement being missed.	Standard service timeframe is within 45 minutes of being missed.	Team Leader Assignee
For Priority 1 and 2, escalations start after ticket is opened for 15 minutes until ticket is moved to assigned status. For Priority 3 and 4, escalations start when ticket is within 30 minutes of service level agreement being missed.	Standard service timeframe is within 30 minutes of being missed.	Business Unit Leader Team Leader Assignee
For Priority 1 and 2, escalations start after ticket is opened for 15 minutes until ticket is moved to assigned status. For Priority 3 and 4, escalations start when ticket is within 15 minutes of service level agreement being missed.	Standard service timeframe is within 15 minutes of being missed.	Group Leader Business Unit Leader Team Leader Assignee

- Service Level Agreement (SLA).
    - Ensono's Client Service Organization (CSO) will provide documentation around all Service Level Agreements (SLA) as well as measured success against such SLAs.

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.

Ensono can comply

b. Client 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.

Ensono can comply

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

Ensono can comply

© 2018 Ensono, LP. All rights reserved.

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

Ensono can comply

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

Ensono can comply

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.

AWS provides clients with the ability to delete their data. However, AWS clients retain control and ownership of their data, and it is the client's responsibility to manage their data.

In addition, it is important that clients understand some important basics regarding data ownership and management in the cloud shared responsibility model:

1. Clients continue to own their data.
2. Clients choose the geographic location(s) in which to store their data—it does not move unless the client decides to move it.
3. Clients can download or delete their data whenever they like.
4. Clients should consider the sensitivity of their data, and decide if and how to encrypt the data while it is in transit and at rest.

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

Ensono complies with all applicable laws. Further, AWS provides the flexibility for clients to move their data to a number of global regions should any issues arise.

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.

Ensono centrally logs all access within the AWS Managed environment and this data is available for clients to review. Ensono only uses the access and permissions necessary to manage the infrastructure.

8.6(E) PRIVACY AND SECURITY

© 2018 Ensono, LP. All rights reserved.

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.

NIST 800-145: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Leveraging AWS, Ensono is able to adhere to NIST 800-145 principles around cloud, as well as leveraging the AWS platform that is already compliant with NIST 800-171. This includes a subset of NIST 800-53 that AWS has leveraged around their FedRAMP audit.

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.

In addition to AWS' government standards, Ensono is:

- SOC 1 Type II and SOC 2 Type II [Security, Availability and Confidentiality] – US and Poland
    - ISO 27001 [Information Security Management System] – UK (in process in US and Poland)
    - ISO 22301 [Business Continuity Management System] – UK
    - ISO 9001 [Quality Management System] – UK
    - ISO 20000 [IT Service Management] – UK
    - PCI DSS AoC – UK

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.

Ensono operates each client independently within the AWS global network. Network segmentation, isolation, as well as geographical separate are all part of the design process. This ensures that "neighbors" are not able to infect or degrade service for other clients.

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

© 2018 Ensono, LP. All rights reserved.

administrators have to stored data. Include information on your hardware policies (laptops, mobile etc.).

AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor:

- Server and network usage
- Port scanning activities
- Application usage
- Unauthorized intrusion attempts.

In addition, these tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a conferencing system is used that supports communication and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. Post-mortems are convened after any significant operational issue, regardless of external impact, and Cause of Error (COE) documents are drafted so the root cause is captured and preventative actions are taken in the future. Implementation of the preventative measures is tracked during weekly operations meetings.

AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks.

The AWS network provides significant protection against traditional network security issues, and you can implement further protection. The following are a few examples:

Distributed Denial Of Service (DDoS) Attacks. AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.

© 2018 Ensono, LP. All rights reserved.

Man in the Middle (MITM) Attacks. All of the AWS APIs are available via SSL-protected endpoints that provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. You can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. We encourage you to use SSL for all of your interactions with AWS.

IP Spoofing. Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port Scanning. Unauthorized port scans by Amazon EC2 clients are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Clients can report suspected abuse via the contacts available on our website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by you. Your strict management of security groups can further mitigate the threat of port scans. If you configure the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. In these cases, you must use appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. For example, a web server must clearly have port 80 (HTTP) open to the world, and the administrator of this server is responsible for the security of the HTTP server software, such as Apache. You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

Packet sniffing by other tenants. It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While you can place your interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same client located on the same physical host cannot listen to each other's traffic. Attacks such as ARP cache poisoning do not work within Amazon EC2 and Amazon VPC. While Amazon EC2 does provide ample protection against one client inadvertently or maliciously attempting to view another's data, as a standard practice you should encrypt sensitive traffic.

Information on Ensono's hardware policies (laptops, mobile etc.) can be found in Ensono's Information Security Policy (please refer to **Ensono Addendum-InformationSecurityPolicy.PDF**).

© 2018 Ensono, LP. All rights reserved.

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

- SOC 1 Type II and SOC 2 Type II [Security, Availability and Confidentiality] – US and Poland
- ISO 27001 [Information Security Management System] – UK (in process in US and Poland)
- ISO 22301 [Business Continuity Management System] – UK
- ISO 9001 [Quality Management System] – UK
- ISO 20000 [IT Service Management] – UK
- PCI DSS AoC – UK

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.

The logging and monitoring of Application Program Interface (API) calls are key components in security and operational best practices, as well as requirements for industry and regulatory compliance. AWS clients can leverage multiple AWS features and capabilities, along with third-party tools, to monitor their instances and manage/analyze log files.

AWS CloudTrail

AWS CloudTrail is a web service that records API calls to supported AWS services in an AWS account, delivering a log file to an Amazon Simple Storage Service (Amazon S3) bucket. AWS CloudTrail alleviates common challenges experienced in an on-premise environment by making it easier for clients to enhance security and operational processes while demonstrating compliance with policies or regulatory standards.

With AWS CloudTrail, clients can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

For information on the services and features supported by AWS CloudTrail, visit the AWS CloudTrail FAQs on the AWS website.

© 2018 Ensono, LP. All rights reserved.

The AWS whitepaper *Security at Scale: Logging In AWS* provides an overview of common compliance requirements related to logging, detailing how AWS CloudTrail features can help satisfy these requirements.

The AWS whitepaper *Auditing Security Checklist for Use of AWS* provides clients with a checklist to assist in evaluating AWS for the purposes of an internal review or external audit.

AWS CloudTrail: Features and Benefits

Some of the many features of AWS CloudTrail include:

Increased Visibility: AWS CloudTrail provides increased visibility into user activity by recording AWS API calls. Clients can answer questions such as, what actions did a given user take over a given time period? For a given resource, which user has taken actions on it over a given time period? What is the source IP address of a given activity? Which activities failed due to inadequate permissions?

Durable and Inexpensive Log File Storage: AWS CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably and inexpensively. Clients can use Amazon S3 lifecycle configuration rules to further reduce storage costs. For example, clients can define rules to automatically delete old log files or archive them to Amazon Glacier for additional savings.

Easy Administration: AWS CloudTrail is a fully managed service; clients simply turn on AWS CloudTrail for their account using the AWS Management Console, the Command Line Interface, or the AWS CloudTrail SDK and start receiving AWS CloudTrail log files in the specified Amazon S3 bucket.

Notifications for Log File Delivery: AWS CloudTrail can be configured to publish a notification for each log file delivered, thus enabling clients to automatically take action upon log file delivery. AWS CloudTrail uses the Amazon Simple Notification Service (Amazon SNS) for notifications.

Choice of Partner Solutions: Ensono is working on a partnership with AlertLogic to further enhance the monitoring and logging capabilities. Additionally, multiple partners including AlertLogic, Boundary, Loggly, Splunk, and Sumologic offer integrated solutions to analyze AWS CloudTrail log files. These solutions include features like change tracking, troubleshooting, and security analysis. For more information, see the AWS CloudTrail partners section.

Log File Aggregation: AWS CloudTrail can be configured to aggregate log files across multiple accounts and regions so that log files are delivered to a single bucket. For detailed instructions, refer to the Aggregating CloudTrail Log Files to a Single Amazon S3 Bucket section of the user guide.

Amazon CloudWatch

© 2018 Ensono, LP. All rights reserved.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications run on AWS. Clients can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by client applications and services, and any log files that applications generate. Clients can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react and keep their application running smoothly.

Clients can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. Clients can send their existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time. This helps clients better understand and operate their systems and applications, and they can store their logs using highly durable, low-cost storage for later access.

LogAnalyzer for Amazon CloudFront

LogAnalyzer allows clients to analyze their Amazon CloudFront Logs using Amazon Elastic MapReduce (Amazon EMR). Using Amazon EMR and the LogAnalyzer application clients can generate usage reports containing total traffic volume, object popularity, a break down of traffic by client IPs, and edge location. Reports are formatted as tab delimited text files, and delivered to the Amazon S3 bucket that clients specify.

Amazon CloudFront's Access Logs provide detailed information about requests made for content delivered through Amazon CloudFront, AWS's content delivery service. The LogAnalyzer for Amazon CloudFront analyzes the service's raw log files to produce a series of reports that answer business questions commonly asked by content owners.

Reports Generated

This LogAnalyzer application produces four sets of reports based on Amazon CloudFront access logs. The Overall Volume Report displays total amount of traffic delivered by CloudFront over the course of whatever period specified. The Object Popularity Report shows how many times each client object is requested. The client IP report shows the traffic from each different client IP that made a request for content. The Edge Location Report shows the total number of traffic delivered through each edge location. Each report measures traffic in three ways: the total number of requests, the total number of bytes transferred, and the number of request broken down by HTTP response code. The LogAnalyzer is implemented using Cascading (http://www.cascading.org) and is an example of how to construct an Amazon Elastic MapReduce application. Clients can also customize reports generated by the LogAnalyzer.

Third Party Tools

© 2018 Ensono, LP. All rights reserved.

Many third-party log monitoring and analysis tools are available on AWS Marketplace.

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

AWS Identity and Access Management (IAM) is a web service that enables AWS clients to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console. With AWS IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

Permissions let you specify who has access to AWS resources and which actions they can perform on those resources. Every AWS Identity and Access Management (IAM) user starts with no permissions. In other words, by default, users can do nothing, not even view their own access keys. To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user), or add the user to a group that has the desired permission.

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.

AWS has implemented various methods of external communication to support its client base and the community. Mechanisms are in place to allow the client support team to be notified of operational issues that impact the client experience. A "Service Health Dashboard" is available and maintained by the client support team to alert clients to any issues that may be of broad impact. The “AWS Security Center” is available to provide you with security and compliance details about AWS. You can also subscribe to AWS Support offerings that include direct communication with the client support team and proactive alerts to any client impacting issues.

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.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

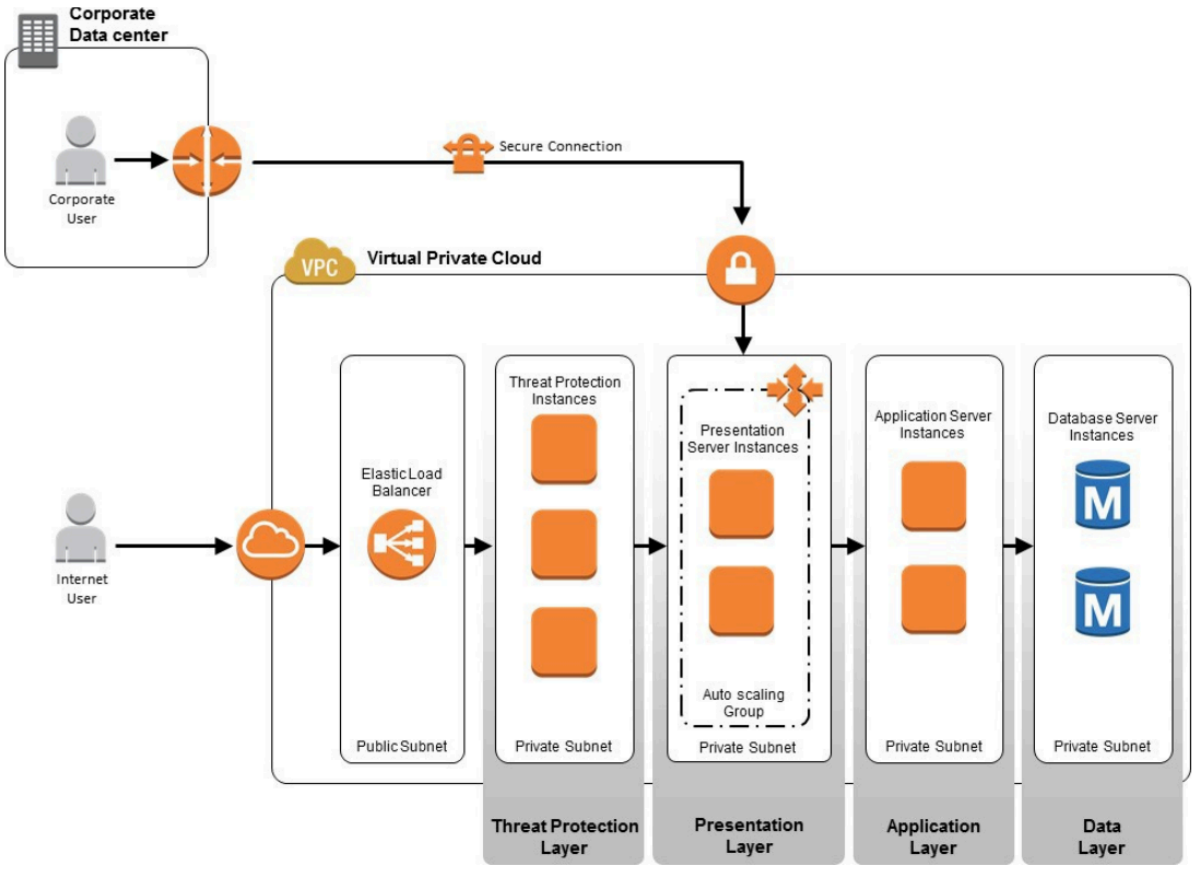
You can easily customize the network configuration for your Amazon Virtual Private Cloud. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application

© 2018 Ensono, LP. All rights reserved.

servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

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).

Reference Architecture for Secure IaaS:



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.

Ensono completes background checks on all employees as part of our standard HR on-boarding process.

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.

© 2018 Ensono, LP. All rights reserved.

AWS clients retain control and ownership of their data, and all data stored by AWS on behalf of clients has strong tenant isolation security and control capabilities. Clients should consider the sensitivity of their data and decide if and how they will encrypt data while it is in transit and while it is at rest.

Securing Data at Rest

There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions to manual, client-side options. Choosing the right solutions depends on which AWS cloud services are being used and client requirements for key management. Information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon Simple Storage Service (Amazon S3) Developer Guide.

Additionally, the *Securing Data at Rest with Encryption* whitepaper provides an overview of the options for encrypting data at rest in AWS cloud services. It describes these options in terms of where encryption keys are stored and how access to those keys is controlled. Both server-side and client-side encryption methods are discussed with examples of how each can be accomplished in various AWS cloud services.

Securing Data in Transit

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers and network traffic between servers.

Services from AWS provide support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

The *AWS Security Best Practices* whitepaper provides greater detail on how to protect data in transit and at rest in the AWS cloud.

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.

Please refer to the answer in Section 8.1.3. For suspected incidents or Data Breaches, Ensono follows our Security Incident Response Plan, which is driven by Ensono's Security Operations Center (SOC). The response times, methodology, and methods of communication are further explained in the document **Ensono Addendum-SecurityIncidentResponsePlan.PDF**.

© 2018 Ensono, LP. All rights reserved.

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.

The client will always maintain control of their data and Ensono's Client Services Organization (CSO) will work with the Purchasing Entity to ensure safe deprovisioning. Ensono is still under full contract, as well as applicable SLAs, until the deprovisioning process is completed and signed off on by the client.

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.

As described above in 8.7.1, Ensono is always under SLA until the contract or deprovisioning project is complete. The client always maintains control to their data and can access it at any time, including deleting or downloading from the AWS infrastructure.

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

Ensono works with clients to design solutions that are not impacted with single points of failure, which is the most common reason for extended downtime. We also use Infrastructure-as-Code provisioning scripts that allow us to leverage other regions and/or Availability Zones within AWS to quickly re-deploy the infrastructure and restore from backups. By leveraging Amazon Machine Images (AMI), we can quickly deploy client applications as well, as they can be part of the automated building process.

b. Suffers an unrecoverable loss of data

In the event of an uncoverable loss of data, the client's system will be rebuilt from our templates, using Infrastructure-of-Code and a combination of Amazon Machine Images (AMI) and restored data from the backup repository or AWS S3 Snapshots.

c. Offeror experiences a system failure

The AWS environment provides the ability to separate compute from storage. In the event of a system failure, the storage can be reattached to a newly instantiated instance, and quickly recover the environment. Amazon's infrastructure has a high level

© 2018 Ensono, LP. All rights reserved.

of availability and provides clients the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal client impact. Data center Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group.

Availability

Data centers are built in clusters in various global regions. All data centers are online and serving clients; no data center is "cold." In case of failure, automated processes move client data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions, as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

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

As described above in "c. Offeror experiences a system failure," the hope is to purposefully design around the potential of a severe system outage. However, if such an outage shall occur, Ensono will use a combination of Infrastructure-as-Code, Amazon Machine Image (AMI), and backups or S3 Snapshots to quickly restore services. Leveraging code instead of humans allows for recoveries in far less than four business hours.

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

RPO and RTOs are part of our design process. Ensono works with our clients to design the appropriate level of RPO and RTO based on the client's need.

Disaster Recovery

The AWS cloud supports many popular DR architectures from "pilot light" environments that are ready to scale up at a moment's notice, to "hot standby" environments that enable rapid failover. With data centers in 12 regions around the world (four in the United States), AWS provides a set of cloud-based DR services that enable rapid recovery of IT infrastructure and data.

8.8.2 Describe your methodologies for the following backup and restore services:

© 2018 Ensono, LP. All rights reserved.

a. Method of data backups

Described below in section "d Ability to recover and restore data within four business hours in the event of a severe system outage"

b. Method of server image backups

Described below in section "d Ability to recover and restore data within four business hours in the event of a severe system outage"

c. Digital location of backup storage (secondary storage, tape, etc.)

Described below in section "d Ability to recover and restore data within four business hours in the event of a severe system outage"

d. Alternate data center strategies for primary data centers within the continental United States

The AWS platform enables a lightweight approach to backup and recovery due, in part, to the following characteristics:

- Computers are now virtual abstract resources instantiated via code rather than being hardware based.
- Capacity is available at incremental cost rather than up-front cost.
- Resource provisioning takes place in minutes, lending itself to real-time configuration.
- Server images are available on demand, can be maintained by an organization, and can be activated immediately.
- These characteristics offer clients opportunities to recover deleted or corrupted data with less infrastructure overhead.

Protecting Configurations Rather Than Servers

The Amazon Elastic Compute Cloud (Amazon EC2) service enables the backup and recovery of a standard server, such as a web server or application server, so that clients can focus on protecting their configuration and the state of data rather than the server itself. This set of data is much smaller than the aggregate set of server data that typically includes various application files, operating system files, temporary files, etc. This change of approach means that regular nightly incremental or weekly full backups can take far less time and consume less storage space.

When a compute instance is started in Amazon EC2, it is based upon an Amazon Machine Image (AMI) and can also connect to existing storage volumes—for example, Amazon Elastic Block Store (Amazon EBS). In addition, when launching a new instance, it is possible to pass user data to the instance that can be accessed internally as dynamic configuration parameters.

© 2018 Ensono, LP. All rights reserved.

A sample workflow is as follows:

Launch a new instance of a web server, passing it the identity of the web server and any security credentials required for initial setup. The instance is based upon a pre-built AMI that contains the operating system and relevant web server application (e.g., Apache or IIS).

Upon startup, a boot script accesses a designated and secured Amazon Simple Storage Service (Amazon S3) bucket that contains the specified configuration file(s).

The configuration file contains various instructions for setting up the server (e.g., web server parameters, locations of related servers, additional software to install, and patch updates).

The server executes the specified configuration and is ready for service. An open-source tool for performing this process called cloud-init is already installed on Amazon Linux AMIs, and is also available for a number of other Linux distributions.

Figure 1 depicts a traditional backup approach and **Figure 2** depicts an Amazon EC2 backup approach.

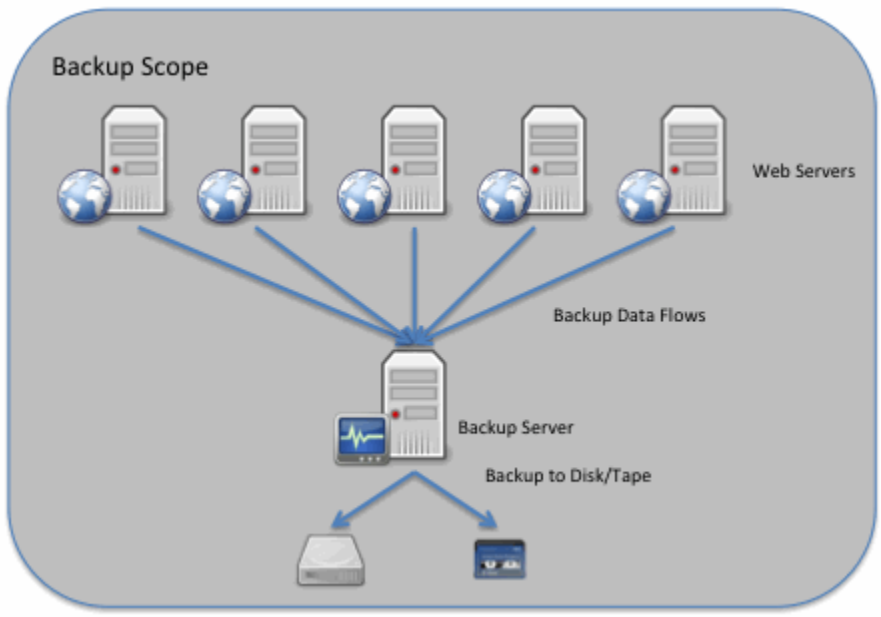


Figure 1 – Traditional Backup Approach

© 2018 Ensono, LP. All rights reserved.

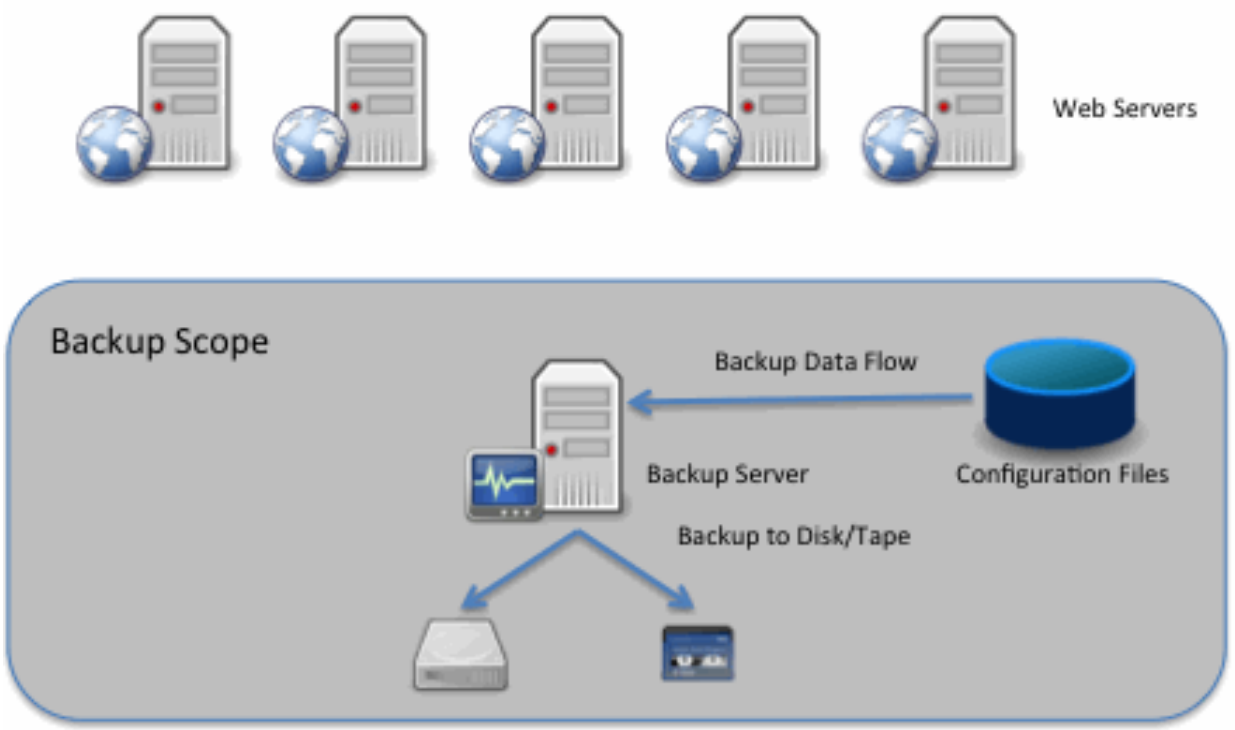


Figure 2 – Amazon EC2 Backup Approach

In this case, there is no need to back up the server itself. The relevant configuration is contained in the combination of the AMI and the configuration file(s). So, the only components requiring backup and recovery are the AMI and configuration file(s).

Amazon Machine Image (AMI)

AMIs that clients register are automatically stored in their account using Amazon EBS snapshots. These snapshots reside in Amazon S3 and are highly durable. This means that the underlying storage mechanism for the AMIs is protected from multiple failure scenarios.

It is also possible to share AMIs between separate AWS accounts. Consequently, clients can create totally independent copies of the AMI by:

- Sharing the original AMI to another specified AWS account controlled by the client.
- Starting a new instance based upon the shared AMI.
- Creating a new AMI from that running instance.

The new AMI is then stored in the second account and is an independent copy of the original AMI. Of course, clients can also create multiple copies of the AMI within the same account.

Configuration Files

© 2018 Ensono, LP. All rights reserved.

Clients use a variety of version management approaches for configuration files, and they can follow the same regime for the files used to configure their Amazon EC2 instances. For example, a client could store different versions of configuration files in designated locations and securely control them like any other code. That client could then back up these code repositories using the appropriate backup cycle (e.g., daily, weekly, monthly) and snapshots to protected locations. Furthermore, clients can use Amazon S3 to store their configuration files, taking advantage of the durability of the service in addition to backing up the files to an alternate location on a regular basis.

Database and File Servers

Backing up data for database and file servers differs from the web and application layers. In general, database and file servers contain larger amounts of business data (tens of GB to multiple TB) that must be retained and protected at all times. In these cases, clients can leverage efficient data movement techniques such as snapshots to create backups that are fast, reliable, and space efficient.

For databases that are built upon RAID sets of Amazon EBS volumes (and have total storage less than 1 TB), an alternative backup approach is to asynchronously replicate data to another database instance built using a single Amazon EBS volume. While the destination Amazon EBS volume will have slower performance, it is not being used for data access and can be easily snapshotted to Amazon S3 using the Amazon EBS snapshot capability.

Disaster Recovery

The AWS cloud supports many popular DR architectures from “pilot light” environments that are ready to scale up at a moment’s notice, to “hot standby” environments that enable rapid failover. With data centers in 12 regions around the world (four in the United States), AWS provides a set of cloud-based DR services that enable rapid recovery of IT infrastructure and data.

General Disaster Recovery/COOP and Backup Requirements and Issues

Some of the minimum needs and requirements in a traditional DR approach are:

- Facilities to house additional infrastructure, including power and cooling.
- Security to ensure the physical protection of assets.
- Suitable capacity to scale the environment.
- Support for repairing, replacing, and refreshing the infrastructure.
- Contractual agreements with an Internet Service Provider (ISP) to provide Internet connectivity that can sustain bandwidth utilization for the environment under a full load.
- Network infrastructure such as firewalls, routers, switches, and load balancers.
- Enough server capacity to run all mission-critical services, including storage appliances for the supporting data, and servers to run applications and back-end

© 2018 Ensono, LP. All rights reserved.

services such as user authentication, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), monitoring, and alerting.

AWS Capabilities for DR/COOP/Backup Solutions

With AWS, clients can eliminate the need for additional physical infrastructure, off-site data replication, and upkeep of spare capacity. AWS uses distinct and geographically diverse Availability Zones (AZs) that are engineered to be isolated from failures in other AZs. This innovative and unique AWS feature enables clients to protect applications from the failure of a single location, resulting in significant cost savings and increased agility to change and optimize resources during a DR scenario.

AWS offers the following high-level DR capabilities:

- **Fast performance** – fast, disk-based storage and retrieval of files
- **No tape** – eliminate costs associated with transporting, storing, and retrieving tape media and associated tape backup software
- **Compliance** – minimize downtime to avoid breaching Service Level Agreements (SLAs)
- **Elasticity** – add any amount of data, quickly. Easily expire and delete without handling media
- **Security** – secure and durable cloud DR platform with industry-recognized certifications and audits

Solution Use Cases

AWS can enable clients to cost-effectively operate multiple DR strategies. **Figure 3** shows a spectrum of scenarios—"backup & restore," "pilot light," "warm standby," and "multi-site"—arranged by how quickly a system can be available to users after a DR event.

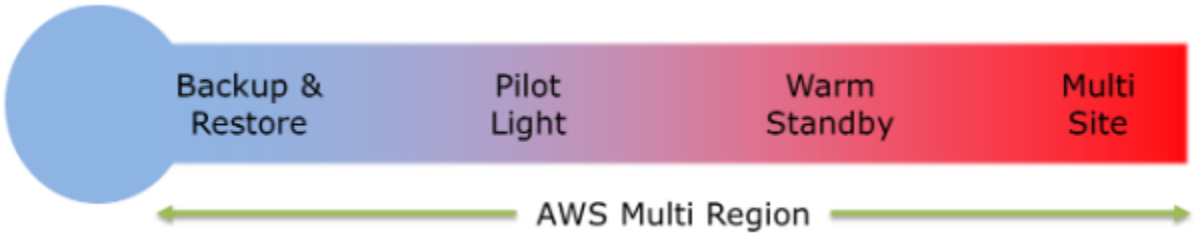


Figure 3 – Spectrum of DR Options.

Each DR option is discussed in more detail below:

© 2018 Ensono, LP. All rights reserved.

Backup and restore: In most traditional environments, data is backed up to tape and sent off-site regularly. Recovery time will be the longest using this method, and lack of automation leads to increased costs. Using Amazon Simple Storage Service (Amazon S3) is ideal for backup data, as it is designed to provide 99.999999999% durability of objects over a given year. Transferring data to and from Amazon S3 is typically done via the network, and it is therefore accessible from any location. Also, with AWS Storage Gateway, clients can automatically back up on-premises data to Amazon S3.

Amazon S3 is designed to provide 99.999999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001% of objects.

Pilot light for simple recovery into AWS warm standby solution: The idea of the pilot light is an analogy that comes from the gas heater. In a gas heater, a small idle flame that's always on can quickly ignite the entire furnace to heat up a house as needed. This scenario is analogous to a backup and restore scenario. However, clients must ensure that they have the most critical core elements of their system already configured and running in AWS (the pilot light). When the time comes for recovery, clients would rapidly provision a full-scale production environment around the critical core.

Warm standby solution in AWS: The term "warm standby" is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. It further decreases recovery time because, in this case, some services are always running. By identifying business-critical systems, clients could fully duplicate these systems on AWS and have them always on.

Multi-site solution deployed on AWS and on-site: A multi-site solution runs in AWS as well as on a client's existing on-premise infrastructure in an active-active configuration. During a disaster situation, an organization can simply send all traffic to AWS servers that can scale to handle their full production load.

DR Resources

There are multiple resources to help organizations start using AWS for a DR/COOP and backup solution:

Read the AWS whitepaper Using AWS for Disaster Recovery

Read the Forrester whitepaper File Storage Costs Less in the Cloud than In-House

Review a sample AWS DR architecture

Review more information on AWS DR capabilities and approaches

8.9(E) DATA PROTECTION

© 2018 Ensono, LP. All rights reserved.

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.

Securing data at rest

There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions to manual, client-side options. Choosing the right solutions depends on which AWS cloud services are being used and client requirements for key management. Information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon Simple Storage Service (Amazon S3) Developer Guide.

Additionally, the *Securing Data at Rest with Encryption* whitepaper provides an overview of the options for encrypting data at rest in AWS cloud services. It describes these options in terms of where encryption keys are stored and how access to those keys is controlled. Both server-side and client-side encryption methods are discussed with examples of how each can be accomplished in various AWS cloud services.

Securing data in transit

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers and network traffic between servers.

Services from AWS provide support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

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.

Ensono is willing to review and sign standard applicable Business Associate Agreements. Such BAAs are subject to review by Ensono's legal counsel.

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.

Ensono does not use or access client's data without permission. We will never use a client's data for data mining.

© 2018 Ensono, LP. All rights reserved.

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.

Ensono leverages AWS' standard SLAs that are used by more than one million AWS clients, including government clients, financial institutions, and healthcare clients, all of which have stringent requirements and demands.

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.

AWS currently provides Service Level Agreements (SLAs) for several products. Due to the rapidly evolving nature of AWS's product offerings, SLAs are best reviewed directly on our website via the links below:

Amazon EC2 SLA: http://aws.amazon.com/ec2-sla/

Amazon S3 SLA: http://aws.amazon.com/s3-sla

Amazon CloudFront SLA: http://aws.amazon.com/cloudfront/sla/

Amazon Route 53 SLA: http://aws.amazon.com/route53/sla/

Amazon RDS SLA: http://aws.amazon.com/rds-sla/

8.11(E) DATA DISPOSAL

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

AWS storage device decommissioning: When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent client data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

8.12(E) PERFORMANCE MEASURES AND REPORTING

© 2018 Ensono, LP. All rights reserved.

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.

All of AWS' services have a minimum of 99.9% availability while most services are 99.99%.

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

AWS currently provides Service Level Agreements (SLAs) for several products. Due to the rapidly evolving nature of AWS's product offerings, SLAs are best reviewed directly on our website via the links below:

- Amazon EC2 SLA: http://aws.amazon.com/ec2-sla/
- Amazon S3 SLA: http://aws.amazon.com/s3-sla
- Amazon CloudFront SLA: http://aws.amazon.com/cloudfront/sla/
- Amazon Route 53 SLA: http://aws.amazon.com/route53/sla/
- Amazon RDS SLA: http://aws.amazon.com/rds-sla/

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.

Ensono will be the single point of contact for all support related issues. Ensono has an Enterprise Support Agreement in place with AWS, so if further escalations are necessary, Ensono will escalate these requests directly to AWS on behalf of the client. Ensono's support organization is available 24x7x365.

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

Shall Ensono/AWS fail to meet any SLAs

1. The client shall declare in writing the specific issue and services impacted.
2. Ensono will investigate with the AWS Technical Account Manager.
3. Appropriate financial compensation will be provided to the client based on the overall length of the outage.

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

AWS has designed their infrastructure to minimize the need for planned downtime. Maintenance activities are typically performed in isolation to remove the need to impact its clients. In the event that maintenance is needed for specific items, such as

© 2018 Ensono, LP. All rights reserved.

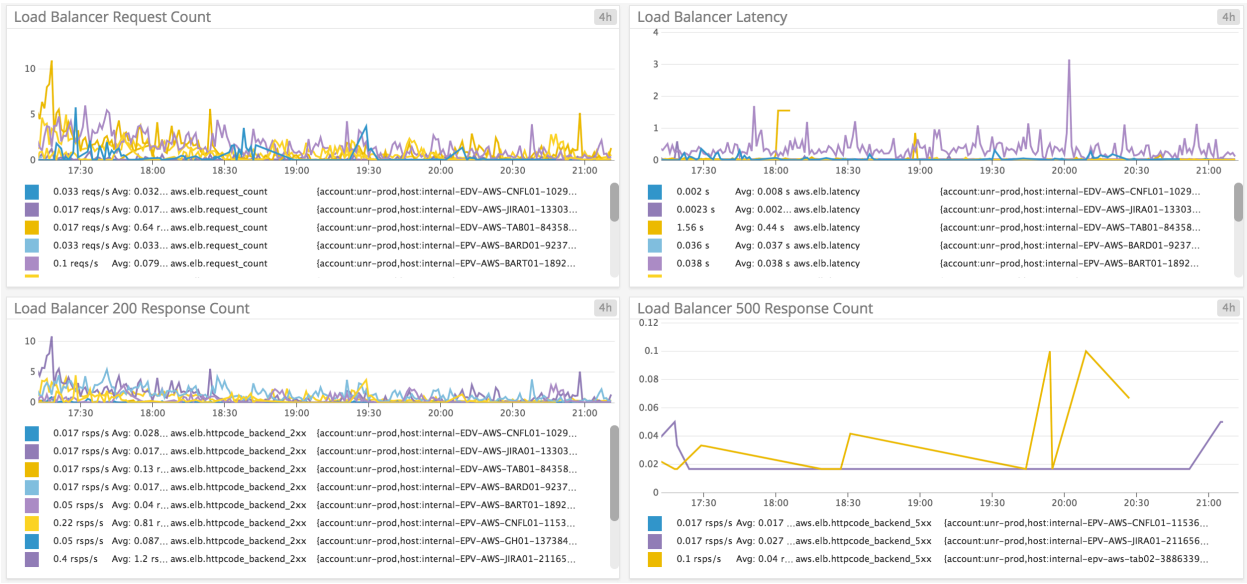
client compute instances, then the client can specify when the maintenance, typically a reboot, takes place.

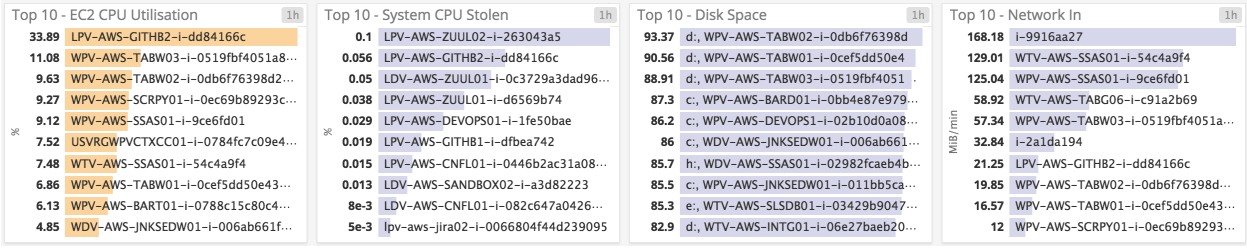
8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Ensono does not provide SLA remedies for disaster recovery (DR) metrics other than the components that are used in the DR solution. For environments that need higher availability and resiliency, Ensono will purpose-build the environment to leverage multiple availability zones. Designing for high availability and resiliency eliminates the needs for a secondary, passive data center.

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.

Ensono provides all reports via a standard performance portal. Sample reports are included below:

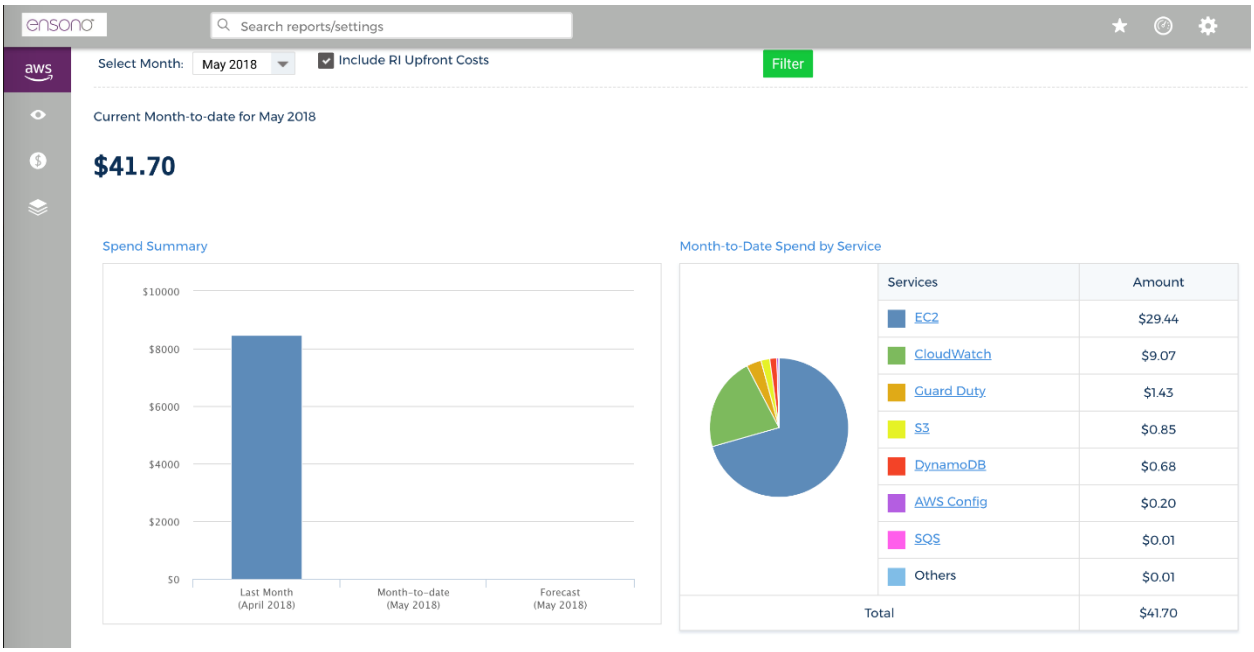


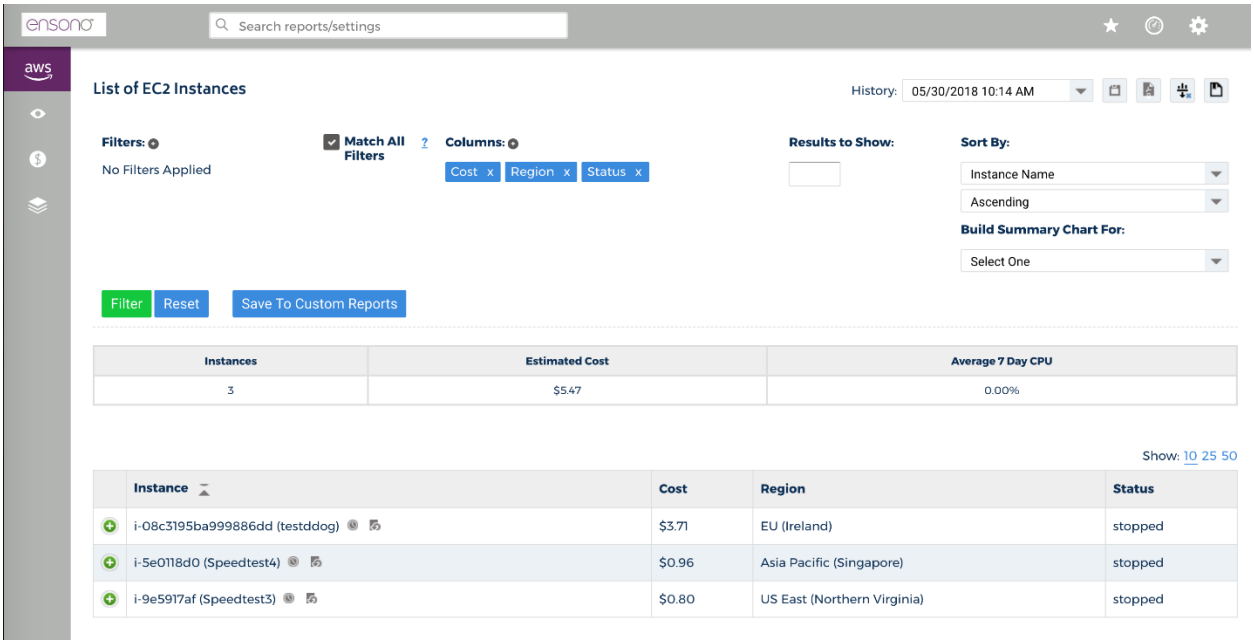


8.12.8 Ability to print historical, statistical, and usage reports locally.

© 2018 Ensono, LP. All rights reserved.

Ensono includes historical reports as well as access to our Insight Cloud Portal. This portal includes billing information, optimization recommendations, and reports based on tags, accounts, availability zones, and much more.





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

Ensono's on-demand deployments are fully supported 24x365.

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

© 2018 Ensono, LP. All rights reserved.

Ensono leverages scripting in conjunction with AWS Auto-Scaling Groups (ASG). Auto-Scaling Groups allow infrastructure to be deployed, automatically, once per-determined triggers, which match the client's business activity, are met, such as heavy CPU/Memory utilization. The ASGs are configured for scale-down activities as well. The result is that the infrastructure will scale up/down as needed without human intervention.

8.13(E) CLOUD SECURITY ALLIANCE

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

a. Completion of a CSA STAR Self-Assessment. (3 points)

b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)

c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)

d. Completion CSA STAR Continuous Monitoring. (5 points)

Ensono is submitting a CSA STAR Registry Self-Assessment: a completed Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B.

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.

Ensono's Client Services Organization (CSO) acts as an escalation path for implementing rush services. Because Ensono leverages automation and orchestration to deploy services, these are typically not an issue to accommodate.

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

Standard services, once requirements are gathered and complete, are delivered in less than 24 hours. These services include: deployment of EC2 Instances, RDS, S3 buckets, adding additional volumes to existing EC2 instances, and Redshift.

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.

Ensono leverages a flexible backup solution that uses S3 Snapshots and Information Lifecycle Management (ILM). This flexible technology allows the client to dictate any retention period needed.

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

© 2018 Ensono, LP. All rights reserved.

The most inherent disaster recovery risk is thinking of the solution as disaster recovery. Ensono works with clients to mitigate this risk by creating solutions that balance traffic between multiple availability zones. This level of high availability and resiliency removes one of the largest risks.

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.

Availability

Data centers are built in clusters in various global regions. All data centers are online and serving clients; no data center is “cold.” In case of failure, automated processes move client data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

You should architect your AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

8.16(E) HOSTING AND PROVISIONING

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

Ensono leverages Terraform to create the environment, including the Virtual Private Cloud (VPC), Network Subnets, Security Groups (SG), Identity Access Management (IAM) roles/policies, load balancers, and EC2 instances, which are leveraged as Amazon Machine Images (AMI). Ansible is used to orchestrate specific Operating System changes at scale with a one-to-many deployment methodology.

8.17.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

© 2018 Ensono, LP. All rights reserved.

Deploying single servers or adding servers to a server farm are done by modifying Terraform Scripts, which are "JSON State Files", or scripts that hold the state of the existing environment. Executing the "build" command will deploy the changes to the environment.

2. Creating and storing server images for future multiple deployments

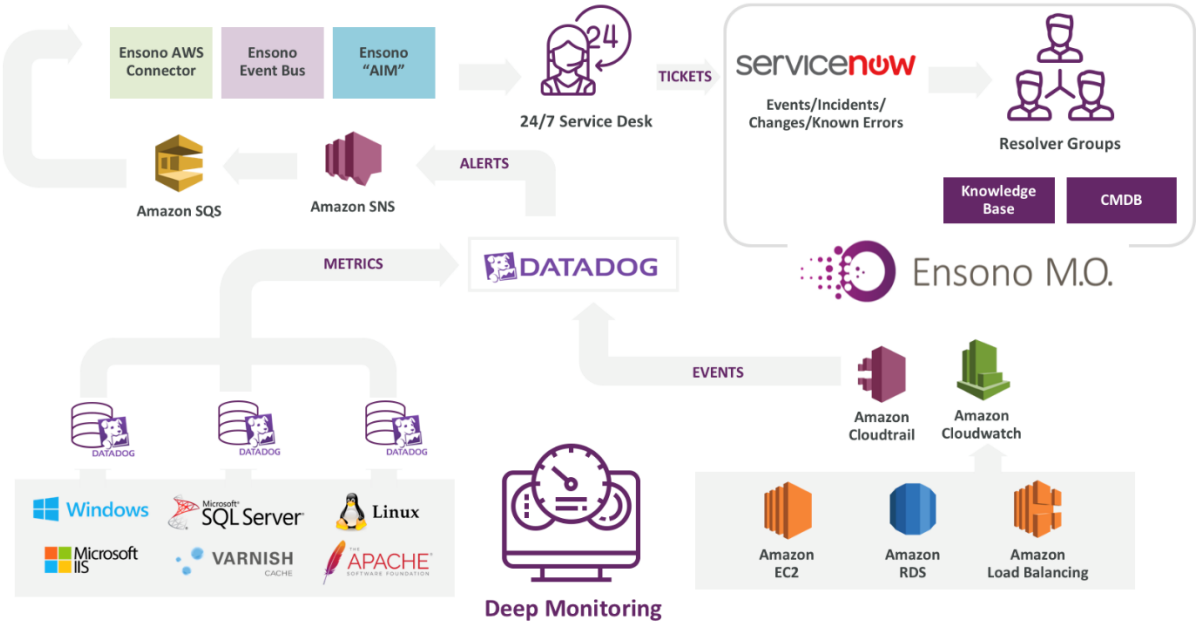
Ensono leverages a combination of Amazon Machine Images (AMI) and Packer to create "gold images" with client-specific builds that can be quickly deployed.

3. Securing additional storage space

Similar to the deployment of new servers, Terraform Scripts can be modified to add additional storage volumes.

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

Ensono leverages AWS CloudWatch and DataDog monitoring events that are enriched and pushed into the intelligent Ensono ITSM platform, called Ensono M.O.



8.17(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.

© 2018 Ensono, LP. All rights reserved.

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.

Ensono has a well-documented POC process to help clients understand how their application will perform against pre-determined success criteria. Depending on the use case, many of these POCs have minimal charges associated with them to allow the client to quickly understand the capabilities of the platform as well as interacting with Ensono as their Managed Services Provider.

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

Ensono provides full on-boarding as part of its standard offering. This includes knowledge around how to open tickets with Ensono, as well as how to interface with Ensono's "Gateway," our portal for full visibility into the environment for maintaining run state. This also includes access to our Cloud Insight Portal that provides clients with detailed billing and reporting options, inventory reports, and customizable reports that focus on chargeback models leveraging AWS Tagging.

8.18(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.

Ensono works with our clients to offer multiple integration options and capabilities. Starting with the AWS infrastructure, there is a large breadth of additional services and capabilities that can be added to the solution. This includes AWS Marketplace applications, API Gateway, as well as Hybrid IT options to leverage the AWS cloud in conjunction with on-premise solutions.

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

Ensono has reference architectures to support many deployments, but we customize each solution for the individual client based on their business and technical needs. Leveraging AWS-trained and certified architects, we work with our clients to understand how to best customize the infrastructure and capabilities of the platform to create a client-tailored solution.

8.19(E) MARKETING PLAN

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

© 2018 Ensono, LP. All rights reserved.

Ensono intends to present its cloud solutions to NASPO ValuePoint and Participating Entities through a multi-touch marketing strategy encompassing multiple platforms:

1) Ensono will issue a press release working with NASPO ValuePoint public relations group to announce the contract award. Ensono has received significant coverage by industry and technology publications in America such as CIO, Network World, TechTarget, CRN and Channel Partners. Ensono has also received coverage in top tier publications including the Wall Street Journal and Fast Company and regional coverage in Crain's Chicago Business and Arkansas Business Journal.

2) Social Media Coverage: Ensono's blog and social media networks such as LinkedIn and Twitter distribute the latest news and hybrid IT insights from our product experts to our 24,000 followers/subscribers. Our marketing efforts are supported by a social media advocacy program that helps extend our brand's reach through our associates' professional network connections. Users from NASPO ValuePoint and participating entities can subscribe to receive the latest cloud solutions content updates.

3) Newsletter distribution to NASPO ValuePoint and participating entities: Ensono Digital Team will send out a quarterly dedicated newsletter linking to the latest articles, white papers, and videos that pertain to this audience.

4) NASCIO Association membership: Ensono is a member of NASCIO and we participate in the spring and fall events and will promote our position as a NASPO contract holder at these events.

5) Events: Ensono regularly participates in industry trade shows such as AWS re:Invent and Microsoft Ignite showcasing our cloud solutions. We will promote that we are a NASPO contract holder.

6) Account-Based Marketing: Ensono will run account-based marketing to the directors and staff of the central procurement offices in the 50 states so they are continually updated on our cloud solutions offerings.

8.20(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.

Ensono is including the following Value-Added services categories:

- Hourly Services for project-based implementations
- Consulting Assessment Services
- Security Management

© 2018 Ensono, LP. All rights reserved.

- Transformation with Ensono Flex

Hourly Services

Clients may acquire Ensono Hourly Services in support of Cloud projects. The representative skills are described below.

- **Project Manager** – manages project resources and schedules and facilitates communications between Ensono and the client
- **Systems Administrator** – provides technical and operational support for operating systems platforms
- **Database Administrator** – provides technical, operational, and applications support for databases
- **Network Engineer** – designs, installs, and configures networks; and provides technical and operational support
- **Security Engineer** – designs, installs, and configures security products; provides technical and operational support; and assists with clients' audit and compliance reviews
- **Infrastructure Architect** – designs infrastructure solutions according to client requirements

Consulting Assessment Services

Ensono's consulting assessment services deliver the following capabilities that are essential in the client's transformation to Cloud:

- Inventory and assessment of IT assets across business
- Design and blue printing of target IT environments
- Mapping out strategies for IT consolidation and optimization
- Creating strategy documents with detailed process of IT migration
- Roadmaps with key milestones and timelines in the migration process

Ensono provides three core assessment packages that are designed to work together or independently.

IT Asset Inventory aims to determine what IT assets you currently have and what recommendations and insights we can offer on this inventory.

Application Dependency Mapping uncovers your application dependencies among servers, which lowers risk, saves time, and brings a common understanding between your application and IT teams.

© 2018 Ensono, LP. All rights reserved.

Target State Design and Migration Plan first determines your existing assets and readiness for upgrade or transformation, and then shows exactly how to transition from current setup to a more rational, efficient, and lower-cost model.

Security Management

Businesses have become almost entirely dependent on the continued availability, accuracy and confidentiality of their data and systems. Our Security Management services give you access to experienced security specialists as a service to bring you IT peace of mind.

Malware Protection Service consists of providing service for malware detection, protection, and incident management. This service seeks to protect against various forms of malware that may threaten the security of server instances.

Vulnerability Management Service helps clients baseline and manage risks due to vulnerabilities in cloud. This service features monthly high-speed IP discovery, fingerprinting, scanning, assessment, and reporting functions. This service supports scanning a wide range of computing platforms and devices including cloud instances, mainframe systems, operating systems, network devices, next generation firewalls, hypervisors, databases, web servers, and more.

Managed Security Information Event Management enables real-time correlation of security information to identify high-risk threats, attacks and security breaches. SIEM combines the automatic prioritization of high-priority incidents with proactive analysis of existing risks due to configuration issues or vulnerabilities

Privileged Session Recording records privileged session activity across all user actions and provides a playback of those user actions. This service is designed to provide oversight and compliance for administrative sessions of Windows-based servers used for secure remote access into client environments.

Security Health Check Advisory Service helps to determine, at a high-level, an organization's compliance with a selection from the fourteen domains of the ISO 27002:2013 standard. The assessment is conducted to a level of rigor that Ensono deems sufficient and appropriate for most purposes. The scope of the assessment will include specific domains and several other key items such as select internal and external vulnerability scanning, as well as other reviews as deemed necessary by Ensono engineers.

Managed Network Intrusion Detection and Prevention delivers deep visibility, security intelligence and superior advanced threat protection. This service combines industry-leading intrusion prevention capabilities and multiple techniques to detect even the most sophisticated network attacks and protect against them. This service is fully-

© 2018 Ensono, LP. All rights reserved.

managed by Ensono providing always-on protection, contextual awareness, security intelligence, event prioritization and reporting.

Managed Malware Defense consists of providing service for Malware Defense, detection, and incident management designed for managed infrastructure and RIM. This service is delivered using Ensono's Malware Defense Management console infrastructure. Malware protection seeks to protect against various forms of malware that may threaten the security of server instances.

Managed Configuration Policy Compliance Auditing Infrastructure Service ensures that managed IT infrastructure assets are compliant with policy and standards. This service is built on a regular process that audits and reports on the configurations and policies of mission critical infrastructure.

Explicit Forward Proxy Essentials retrieves information from an untrusted network and returns it to the requestor, or operating system that resides in a trusted zone. This service enables the ability to control maintenance downloads by whitelisting URLs and methods that can be used.

Transformation with Ensono Flex

Ensono is trusted by some of the world's most successful companies because we deliver complete hybrid IT solutions and governance customized to each client's IT journey. Ensono Flex provides the Client with the mechanism to transfer their IT consumption across multiple platforms within a Hybrid environment.

The value proposition of Ensono Flex is based on the following premises:

1) Transformation to Cloud often requires the continued upkeep of the Client's legacy systems until all systems can be successfully migrated.
2) Clients who implement best of breed Cloud solutions will typically have multiple Cloud platforms deployed within their enterprise.

The benefits of Ensono Flex include:

- Flexibility and ease of transformation by enabling access to various hybrid platforms
- Flexibility formalized with contractual "scale up/scale down" language
- Transparency delivered with P x Q service catalog
- No penalties for shifting workloads across Ensono platform, from legacy to public cloud

© 2018 Ensono, LP. All rights reserved.

The services below can be part of an Ensono Flex offering that provides value-added complementary services to the proposed Managed AWS IaaS.

Managed z/OS provides an Ensono hosted z/OS platform in the Client's data center or in an Ensono data center. Ensono service fees would include the hosting processor and attached storage, IBM and 3rd party software, technical and operational support services, and optional disaster recovery services.

Managed IBM i provides an Ensono managed IBM i platform in the Client's data center or in an Ensono data center. Depending on the data center used, the workload could be hosted on a dedicated or multi-tenant processor, and processor and software can be either client- or Ensono-owned. Ensono would provide technical and operational support services, including security, with HA and DR options available.

Managed Server Infrastructure provides an Ensono managed Windows, Unix/Linux, VMware platform with numerous options for storage tiers, security, backup, HA and DR, and support and management tiers.

Managed Azure provides management of a client's Azure infrastructure on which they host their applications and services.

- Ensono's Azure Go-Live is a suite of services that enables organizations to examine the suitability of their IT environment for migration Microsoft Azure. It will assess the infrastructure and the applications that use it and provide a migration plan that digitally transforms it from a traditional on-premises data center to Azure.
- Ensono's Azure Platform Managed Service provides Azure core fabric management and monitoring, edge security, and Azure fabric patch management.
- Ensono's Azure Managed IaaS Virtual Machine Managed Service provides OS-Level and below management of all VMs under the service including OS patching, OS anti-malware, business continuity and disaster recovery and backup management
- Ensono's Azure Managed PaaS Services provide fully-managed platform management of the following Azure platforms:
  - Azure SQL
  - Azure app service environments
- Ensono's Azure DevOps Hours provides a way for customers to integrate their existing business services with Azure's ever growing and changing public cloud platform. Examples of DevOps activities are: integrating development source control with Azure, building new automation scripts for business processes, augmenting the customer's existing development practice with new types of DevOps processes.

© 2018 Ensono, LP. All rights reserved.

Ensono Flex will contractually facilitate the financial transfer of capacity from above platforms to the proposed Ensono AWS capacity within the term of the Client's agreement with Ensono.

8.22(E) SUPPORTING INFRASTRUCTURE

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

Ensono does not require any additional infrastructure to support our solutions. We leverage Enterprise-grade software solutions to support our solutions, such as Ansible Tower, BitBucket, and Terraform. We have secure, multi-tenant repositories established for each individual account.

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

Ensono bears the cost of this infrastructure as part of our service offering.

© 2018 Ensono, LP. All rights reserved.

Attachment E
Service Level Agreement

TABLE OF CONTENTS

General Provisions

1. General

This Exhibit and Schedule 1 (Critical Service Levels, Key Performance Indicators (KPIs) and Measuring Methodologies and Tools) attached hereto and incorporated herein, sets forth the agreement between the parties relating to Service Levels and Key Performance Indicators, against which Ensono's performance of the Services will be measured. Ensono will perform each Service for which a Service Level or Key Performance Indicator has been established in accordance with the terms of this Exhibit.

2. Definitions

Capitalized terms used in this Exhibit and not defined herein will have the meaning set forth in the Agreement.

"**At Risk Amount**" means, for any calendar month during the Term, ten percent (10%) of the Monthly Charges, which is the aggregate amount that Ensono will have at risk for Critical Service Level Credits as set forth in Schedule 1.

"**Critical Service Level**" means a measurable aspect of performance specified in Schedule 1 with respect to certain Services for which a Service Level Credit may be payable (i.e., "Availability"). Critical Service Levels shall only apply to production environments.

"**Critical Service Level Metric**" means the numerical measurement for a Critical Service Level (i.e., 99.9%).

"**Critical Service Level Credit Weighting Allocation**" means the percentage specified in Schedule 1 as "Allocation" with respect to each Critical Service Level. The sum of the Critical Service Level Credit Weighting Allocation percentages will equal one hundred percent (100%) and each Critical Service Level Credit Weighting Allocation will be subject to the limitations described in Schedule 1.

"**Earnback Credit**" means a credit to be applied to Ensono to offset any otherwise applicable Service Level Credit if, during the Earnback Period, Ensono achieves a Critical Service Level Metric equal to or greater than the applicable Minimum Service Level(s) in effect during the month in which the related Service Level Failure occurred.

"Earnback Period" means the one (1) month period immediately following a month in which a Service Level Failure occurs .

"Ensono Outages" means the cumulative total unavailability for the Service Environment, as reported by Severity 1 Incident tickets, during the Reporting Window within the Measurement Window of the Service Environment, excluding client outages and planned maintenance.

© 2019 Ensono, LP. All Rights Reserved

"**Excluded Event**" means any event that adversely impacts the Service that is caused by (a) the acts or omissions of Client, its employees, customers, contractors or agents; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by Ensono or its designees; (c) force majeure events; (d) Scheduled or emergency maintenance; (e) any suspension of Service pursuant to the Agreement; (f) the unavailability of required Client personnel, including as a result of any failure to provide Ensono with accurate, current contact information; (g) failure of Client to authorize Ensono to perform recommended changes or maintenance; (h) configurations, equipment or services not supported by Ensono; (i) a third party hardware/software bug that does not have a patch; (j) hardware and software for which maintenance is no longer available; or (k) hardware and software without a maintenance agreement.

"Go Live Date" means the date Ensono notifies Client that Ensono has completed all applicable onboarding / transition Services.

"Key Performance Indicator" or **"KPI"** means a performance metric that is not eligible for a Service Level Failure or Service Level Credit but will still be measured and reported by Ensono.

"**Minimum Service Level**" means the level of performance specified in Schedule 1 as "Minimum" for each Service for which a Critical Service Level Metric is established.

"**Monthly Charges**" means the total of Ensono monthly recurring charges (excluding any non-recurring or one-time charges) for its performance of the Services described in this SOW for a single calendar month.

"Measurement Window" means the periodic evaluation and reporting frequency identified for each individual Critical Service Level as specified in Schedule 1.

"Reporting Window" means a calendar month or other period of time as specified in Schedule 1.

"Resolution Time" means the difference between the time the first resolver group(s) receives a ticket for resolution and the time when Ensono resolves the incident or provides a work-around for the incident.

"Response Time" means the difference between the time an incident ticket is submitted and the time the first resolver group(s) accepts a ticket for resolution.

"Service Environment" means any collection or aggregation of two (2) or more Ensono products that are designed to perform in accordance with this SOW. Service Environment may include (without limitation) data center facilities, compute hardware and software (Operating System, Database, Middleware), network and storage used to provide Services.

"Service Environment Availability" means the Client can access and use the material features and functions of the Service in accordance with this SOW. The percentage availability calculation formula measured over the Measurement Window, as follows (where "A" = Service Environment

© 2019 Ensono, LP. All Rights Reserved

Availability, "T" = Total Available Service Time (minutes), and "O_{EA}" = Ensono Outages): **A** = (**T** – O_{EA}) x 100% / **T**

"**Service Level Credit**" means a credit in an amount calculated in accordance with Section 3 (Overview of Service Level Credit Process for Service Level Failures) which will be credited to Client by Ensono in connection with Service Level Failures.

"**Service Level Failure**" means, with respect to Critical Service Levels, each month during the Term that Ensono performs a Service at a level below the applicable Minimum Service Level for reasons other than an Excluded Event.

"Service Level Objective" means performance metrics designed to be used during a transition or benchmarking process, which are not eligible for Service Level Credits.

"**Service Level Termination Event**" is defined in Section 10 (Service Level Termination Events) hereof.

"Total Available Service Time" means, the total time in the relevant Reporting Window (i.e.: Monthly Reporting Window: 43,800 minutes of Total Available Service Time = 30.41 calendar days X 24 hours per day X 60 minutes per day).

3. Overview of Service Level Credit Process for Service Level Failures

If a Service Level Failure occurs in any calendar month during the SOW Term (subject to the terms of this Exhibit), Ensono shall provide a Service Level Credit to Client in accordance with this Section 3. Ensono may earn back an applicable Service Level Credit in accordance with Section 4 (Invoicing and Earnback Credits). Ensono's performance with respect to each Critical Service Level will be measured in accordance with the reports described in Section 5 (Reporting).

Calculation. For each Service Level Failure, Ensono will provide to Client a Service Level Credit computed in accordance with the following formula:

Service Level Credit = **A x B**

Where:

A = the Critical Service Level Credit Weighting Allocation percentage specified in Schedule 1 for the applicable Critical Service Level; and

B = the At Risk Amount for the month in which the Service Level Failure occurs.

For example, assume that Ensono fails to meet the Minimum Service Level with respect to "P1 Incident Response" (i.e., a Service Level Failure). Assume further that Ensono's Monthly Charges for Services for the month in which the Service Level Failure occurred were $100,000, and the At Risk Amount is 10% or $10,000. Assume further the Critical Service Level Credit Weighting

© 2019 Ensono, LP. All Rights Reserved

Allocation for P1 Incident Response is 5%. The Service Level Credit due to Client for such Service Level Failure would be $500 and is computed as follows:

A = 5% (the Critical Service Level Credit Weighting Allocation percentage),

multiplied by

B = $10,000 ($100,000 Monthly Fee X 10% At Risk Amount),

equals $500.

Limitations. The total amount of all Service Level Credits credited to Client for Service Level Failures in any single calendar month shall not exceed the At Risk Amount for such month. If more than one Service Level Failure occurs in a single month, the sum of the corresponding Service Level Credits will be credited to Client as set forth in this Exhibit, provided, however, that if a single incident results in the failure of Ensono to meet more than one Critical Service Level, then Ensono will issue the largest single Service Level Credit amount and Client shall not be eligible for additional Service Level Credits for the other related failures.

4. Invoicing and Earnback Credits

In the event of a Service Level Failure, if Ensono fails to achieve an Earnback Credit during the Earnback Period, Ensono will apply the applicable Service Level Credit to the Client's account no later than the second monthly invoice following the applicable Earnback Period. In the event Client earns a Service Level Credit in the final month of the Term, Ensono shall pay to Client the amount of such Service Level Credit within thirty (30) days after the effective date of the termination or expiration of the SOW. Notwithstanding the foregoing, in no event shall Client be entitled to a Service Level Credit if the applicable SOW is terminated or expires prior to the conclusion of the applicable Earnback Period.

5. Reporting

Each month Ensono will issue a report for the preceding month in which Ensono will (i) notify Client of any Service Level Credits to which Client is entitled and (ii) describe any Service Level Failures that occurred. In addition to this standard monthly Service Level report, within twenty (20) business days following the end of each month, Ensono will provide Client an additional report that details (a) Ensono's monthly performance with respect to each Critical Service Level Metric for each month during the last twelve (12) months (or rolling average when in the first twelve (12) months of the applicable Service term), and (b) the total dollar amount of all Service Level Credits earned by Client during the prior month and during the last twelve (12) months.

6. Establishing Critical Service Level Metrics and Minimum Service Levels

FOR HOSTED SOLUTIONS:
The Critical Service Level Metrics and the corresponding Minimum Service Levels are identified in Schedule 1.

© 2019 Ensono, LP. All Rights Reserved

FOR REMOTE INFRASTRUCTURE MANAGEMENT (RIM) SOLUTIONS:
The Critical Service Level Metrics are identified in Schedule 1 and the Minimum Service Levels for each Critical Service Level Metric will be established in one of the following ways:

During the benchmark measurement period below, Ensono will establish Service Level Objectives (SLOs) listed in Schedule 1, to promote service and quality targets to the Client and its end users. SLO metrics are not subject to Service Level Credits or any other remedies.

(i) Where at least nine (9) months of verifiable performance measurements exist for a particular Service, the Minimum Service Level for such Critical Service Level will be equal to the average performance achieved during the two (2) lowest months of such nine (9) month period or the SLO targets whichever is lower; or

(ii) Where there are not at least nine (9) months of verifiable service measurements for a particular Service, Ensono will measure and, on a monthly basis, document its actual performance of such Services for nine (9) consecutive months. The Minimum Service Level will be equal to the average of the documented monthly performance achieved during the two (2) lowest months of such nine (9) month period or the SLO targets whichever is lower.

7. Reclassification of Service Level and Modification of Allocation of Pool Percentages

Reclassification of Service Levels. Client may reclassify any Service Level (e.g., from KPI to Critical Service Level or from Critical Service Level to KPI) upon 30 days' notice and no more than twice a year and no sooner than six months after the Effective Date, and by sending written notice to Ensono.

Modifications of Allocation of Pool Percentages. When reclassifying a Critical Service Level, Client's notice shall include an appropriately modified Critical Service Level Credit Weighting Allocation for the affected Critical Service Level(s), provided, however, that the total Allocation of Pool Percentages shall not exceed the amount noted in the Service Level Credit Weighting Allocation definition in Section 2.

8. Public Clouds (AWS and Azure)

FOR PUBLIC CLOUD SOLUTIONS:
Managed AWS:
Client's sole and exclusive remedy for any Service quality or performance deficiency or failure of any kind will be as set forth in the SLA located at https://aws.amazon.com/legal/service-level-agreements/ which may be modified from time to time. Such SLA (and any related Service Credits), however, shall not apply until the date six (6) weeks following the Go Live Date; thereafter, Service Credits will be issued no later than two (2) months following the month in which the Service Level Failure occurred. All performance calculations and applicable Service Credits are based on Ensono records and data unless Client can provide Ensono with clear and

© 2019 Ensono, LP. All Rights Reserved

convincing evidence to the contrary within thirty (30) days following Client's receipt of the invoice containing the applicable Service Credit.

Managed Azure:
Client's sole and exclusive remedy for any Service quality or performance deficiency or failure of any kind will be as set forth in the SLAs available at https://azure.microsoft.com/en-us/support/legal/sla/,together with any additional SLAs set forth in the applicable Service Order or SOW. Such SLA (and any related Service Credits), however, shall not apply until the date six (6) weeks following the Go Live Date; thereafter, Service Credits will be issued no later than two (2) months following the month in which the Service Level Failure occurred. All performance calculations and applicable Service Credits are based on Ensono records and data unless Client can provide Ensono with clear and convincing evidence to the contrary within thirty (30) days following Client's receipt of the invoice containing the applicable Service Credit.

9. Performance Exceptions

In no event will Ensono be responsible, or will Client be eligible to receive any Service Level Credits, to the extent Ensono's failure to achieve a Critical Service Level is due to an Excluded Event. Client will not be eligible to accrue any otherwise applicable Service Level Credits if Client is in material breach of the Agreement at the time the Service Level Failure occurred, nor will Client be entitled to receive any otherwise available Service Level Credits if Client is in material breach of the Agreement at the time the Service Level Credit is to be issued, provided that the Service Level Credit will be issued once such material breach has been cured, if such breach is cured prior to termination of the SOW.

This Service Level Agreement provides Client's sole and exclusive remedies for any failure to meet the Critical Service Levels. These remedies are as follows:

> *(i) In the event of a Service Level Failure that does not constitute a Service Level Termination Event, as Client's sole and exclusive remedy for such Service Level Failure, Client shall be entitled to receive the applicable Service Level Credits, subject to the terms of this Exhibit; and*
>
> *(ii) In the event of a Service Level Termination Event, Client shall be entitled to pursue the remedies described in Section 10 (Service Level Termination Events) below.*

To clarify, such sole and exclusive remedies shall not apply to breaches of unrelated obligations under the Agreement such as infringement, confidentiality, etc.

10. Service Level Termination Events

A **"Service Level Termination Event"** shall be deemed to have occurred if Ensono suffers four (4) Service Level Failures due to a failure to achieve the applicable Minimum Service Level for the same Critical Service Level in any rolling six (6) month period.

© 2019 Ensono, LP. All Rights Reserved

In the event of a Service Level Termination Event, Client may either (i) accept the applicable Service Level Credits, in which event such Service Level Credits shall represent Client's sole and exclusive remedy for the applicable Service Level Termination Event, or (ii) decline the applicable Service Level Credits by delivering Ensono written notice not later than thirty (30) days following Client's receipt of the invoice containing the Service Level Credits indicating that Client intends to decline the applicable Service Level Credits and terminate, in whole, this SOW. If Client declines the applicable Service Level Credits and elects to terminate this SOW, Ensono agrees to reimburse Client for its reasonable and documented out-of-pocket costs to transition the Services in-house or to another service provider not to exceed the initial installation costs for the terminated Services paid by Client to Ensono, subject to the terms of the Agreement.

11. Improvement Plans for Critical Service Level

If Ensono fails to meet any Minimum Service Level(s), Ensono will promptly provide to Client a written plan, subject to Client review, for improving Ensono's performance to meet or exceed the applicable Minimum Service Level(s). Following the implementation of such plan, Ensono will provide to Client monthly status reports containing progress updates until such time as Ensono's performance is in compliance with the applicable Minimum Service Level.

12. Commencement of Obligations

The obligations set forth herein shall commence upon the date one (1) month following the Go Live Date, unless otherwise specified in Schedule 1. The dates used in the column "Measure Begins" represent when Ensono will be responsible for Service Level Credits for any Service Level Failures, subject to the terms of this Exhibit.

13. Stabilization Periods.

During the term of the Services, Ensono or the Client may make changes to hardware or software that affect Ensono's ability to meet the Critical Service Levels. When such changes arise, a performance ramp period shall apply (each, a **"Stabilization Period"**). The Client shall work with Ensono reasonably and in good faith to agree upon:

- The length of the Stabilization Period and
- Any related changes to the previously established service level metrics.

By way of example but not limitation, the following changes may require a Stabilization Period:

- major release upgrades to the software in the applicable environment;
- the addition of Third Party Software to the applicable environment;
- the addition of additional modules to the applicable environment; or
- major functionality changes to the applicable environment.

For any change not listed above, the parties shall work in good faith to agree upon whether a Stabilization Period is required and as to the length of such period.

© 2019 Ensono, LP. All Rights Reserved