Contract #: AR3108

STATE OF UTAH COOPERATIVE CONTRACT

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

Include Information Management, Inc. DBA i2m
Name

600 West Germantown Pike Suite 400
Street Address

Plymouth Meeting PA 19462
City *State* *Zip*

Vendor # VC226571 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact *Name:* Ahmed Attalla *Phone Number:* 267-240-9097 *Email:* ahmeda@i2m.cloud

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: Monday, March 11, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

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

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

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

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

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

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

CONTRACTOR

3/11/19
Contractor's signature Date

STEVEN GRZYWINSKI PRES/CTO
Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes
Christopher Hughes (Mar 13, 2019) Mar 13, 2019
Director, Division of Purchasing Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

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

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

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

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

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

10. Defaults and Remedies

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

(1) Nonperformance of contractual requirements; or

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

(3) Any certification, representation or warranty by Contractor in response to the

solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

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

13. Indemnification

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

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

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

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

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

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

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

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and

reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

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

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

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

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

aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

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

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor’s general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor’s liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity’s rights and Contractor’s obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

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

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

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

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

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

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

19. Ordering

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

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

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

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

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

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

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

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

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

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

20. Participants and Scope

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26. Records Administration and Audit.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Services it acquires from this Master Agreement.

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

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

32. Transition Assistance:

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

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

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

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

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

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ValuePoint, Contractor shall provide a copy of any such provisions.

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

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

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

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

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

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

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

- 10 days after the effective date of termination, if the termination is in accordance with the contract period

- 30 days after the effective date of termination, if the termination is for convenience

- 60 days after the effective date of termination, if the termination is for cause

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

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

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

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

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

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

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

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

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

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

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

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

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

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

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

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

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

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

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

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

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

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

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

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

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

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

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

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

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

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

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

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

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

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

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

a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

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

8. Background Checks:

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

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

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

9. Access to Security Logs and Reports:

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

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

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

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

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

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

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

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

8. Background Checks:

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

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

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

9. Access to Security Logs and Reports:

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

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

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

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

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

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

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

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

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

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

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

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

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

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

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

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

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

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

1.2 Risk Categorization.*

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

Service Model:	**Low Risk Data**	**Moderate Risk Data**	**High Risk Data**	**Deployment Models Offered:**
SaaS	AWS	AWS	AWS	•Private cloud •Public cloud •Hybrid cloud •Community cloud
SaaS	CloudBerry	CloudBerry	CloudBerry	•Private cloud •Public cloud •Hybrid cloud
SaaS	DUO	DUO	DUO	•Public cloud
SaaS	Druva	Druva	Druva	•Private cloud •Public cloud •Hybrid cloud
SaaS	CloudHealth	CloudHealth	CloudHealth	•Public cloud
SaaS	Trend Micro	Trend Micro	Trend Micro	•Public cloud
IaaS	AWS	AWS	AWS	•Private cloud •Public cloud •Hybrid cloud •Community cloud
PaaS	AWS	AWS	AWS	•Private cloud •Public cloud •Hybrid cloud •Community cloud

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

2.1 Deployment Models.

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

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor Name: Include Information Management, Inc. DBA i2M

Pricing Notes

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

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

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

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

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

Cloud Service Model: Infrastructure as a Service (IaaS)

Description	Minimum Discount % Off
IaaS Minimum Discount % * (applies to all OEM's offered within this IaaS model)	4.50%
Average IaaS OEM Discount Off	**4.50%**

Cloud Service Model: Platform as a Service (PaaS)

Description	Discount
PaaS Minimum Discount % * (applies to all OEM's offered within this PaaS model)	4.50%
Average PaaS OEM Discount Off	**4.50%**

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
CloudHealth	1.00%
DUO	5.00%
Druva	10.00%
CloudBerry	10.00%
Trend Micro	8.00%
Amazon Web Services (AWS)	4.50%
Average SaaS OEM Discount Off	**6.42%**

Additional Value Added Services

	Onsite Hourly Rate		Remote Hourly Rate	
Item Description	**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services	$ 125.00	$ 150.00	$ 100.00	$ 125.00
Professional Services				
Deployment Services	$ 275.00	$ 300.00	$ 250.00	$ 275.00
Integration Services	$ 275.00	$ 300.00	$ 250.00	$ 275.00
Consulting/Advisory Services	$ 275.00	$ 300.00	$ 250.00	$ 275.00
Architectural Design Services	$ 275.00	$ 300.00	$ 250.00	$ 275.00
Statement of Work Services	$ 90.00	$ 110.00	$ 80.00	$ 100.00
Partner Services	$ 200.00	$ 250.00	$ 175.00	$ 225.00
Training Deployment Services	$ 200.00	$ 250.00	$ 175.00	$ 200.00
Other Professional Services	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Cloud Account Review and Management	$ 275.00	$ 300.00	$ 250.00	$ 275.00
Cloud Services Migration, Installation, Implementation, Programming Level 1	$ 175.00	$ 200.00	$ 150.00	$ 175.00
Cloud Services Migration, Installation, Implementation, Programming Level 2	$ 225.00	$ 250.00	$ 200.00	$ 225.00
Cloud Services Migration, Installation, Implementation, Programming Level 3	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Cloud Services Account Management, Maintenance and General Support Level 1	$ 175.00	$ 200.00	$ 150.00	$ 175.00
Cloud Services Account Management, Maintenance and General Support Level 2	$ 225.00	$ 250.00	$ 200.00	$ 225.00
Cloud Services Account Management, Maintenance and General Support Level 3	$ 250.00	$ 300.00	$ 225.00	$ 275.00

Attachment C - Pricing Discounts and Schedule

Contractor Name: Include Information Management, Inc. DBA i2M

Cloud Services General Training Level 1	$ 100.00	$ 120.00	$ 90.00	$ 110.00
Cloud Services General Training Level 2	$ 150.00	$ 175.00	$ 125.00	$ 150.00
Cloud Services General Training Level 3	$ 175.00	$ 200.00	$ 150.00	$ 175.00
Cloud Services Disaster Recovery and Business Contunity Maintenence	$ 125.00	$ 150.00	$ 100.00	$ 125.00
Cloud Services Disaster Recovery and Business Contunity Testing	$ 175.00	$ 225.00	$ 150.00	$ 200.00
Cloud Services Disaster Recovery and Business Contunity Implmentation, Configuration and Planning	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Enterprise Solutions Associate Level 1	$ 175.00	$ 200.00	$ 150.00	$ 175.00
Enterprise Solutions Architect Level 2	$ 225.00	$ 250.00	$ 200.00	$ 225.00
Enterprise Solutions Architect Level 3	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Cloud Services Networking Level 1	$ 175.00	$ 200.00	$ 150.00	$ 175.00
Cloud Services Networking Level 2	$ 225.00	$ 250.00	$ 200.00	$ 225.00
Cloud Services Networking Level 3	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Cloud Dev/Ops Services	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Cloud Security Optmization	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Cloud Cost Optmization Services	$ 250.00	$ 300.00	$ 225.00	$ 275.00
Cloud Services Account Creation Post Implementation	$ 150.00	$ 175.00	$ 125.00	$ 150.00
General Emergency/Rush Services	$ 250.00	$ 300.00	$ 225.00	$ 275.00

	Deliverable Rates	
	NVP Price	Catalog Price
N/A	N/A	N/A

NASPO VALUEPOINT

Business Information 6
Utah Solicitation Number SK18008
Cloud Solutions

July 6th, 2018, 3:00 PM

Include Information Management, Inc.
DBA
(i2m)

600 West Germantown Pike, Suite 400, Plymouth Meeting, PA 19462

Business Information 6

General Information			
RFP Title and Number	RFP Manager	RFP Lead	RFP Contact
Cloud Solutions SK18008 NASPO ValuePoint	Ahmed Attalla ahmeda@i2m.cloud (267) 240-9097	Solomon Kingston, State Contract Analyst State of Utah, Division of Purchasing	Solomon Kingston skingston@utah.gov (801) 538-3228

Document Preparation Information		
Primary Author	Date	Organization Name
Ahmed Attalla Secondary Author Steven Grzywinski	June 1st , 2018	i2m i2m.cloud Include Information Management Inc.
Phone Number	E-mail	Attached Work Order / Invoice
267-240-9097	ahmeda@i2m.cloud	n/a

6 BUSINESS INFORMATION

6.1 (M)(E) BUSINESS PROFILE

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

Response:

Year started

i2m has been in business since 2005

Organizational Structure

i2m team

- Sales: 4 members
- Marketing: 5 members
- Procurement: 5 members

- Accounting: 3 members
- Executive Management: 3 members

Steve Grzywinski: President and CTO

- Roles: Executive Account Manager, Sales, Marketing, Billing and Technical Contact

Scott Miller: COO

- Roles: Executive Account Manager, Sales, Marketing, Billing and Operations Contact

Ahmed Attalla: President of i2m.cloud

- Roles: Executive Account Manager, Primary Sales, Marketing, Billing, Technical Contact

Client Base and Market Focus and Region

i2m’s client base compromises of the two sectors:

Commercial

In our commercial sector we cater to Law practices, Medical practices, Financial firms, Investment and Capital Management firms, Aerospace, Metal and Medical Manufactures and Distributors.

Public Sector

In our Public Sector we cater to small and large non-profit organizations, City, State and Federal Government Agencies.

Commercial Region Focus: US and EU

Public Sector Region: US

Growth over the last three (3) years

Financials show this growth in detail but approximately 50% growth over 3 years up to the current month. i2m's sales grew at an average annual rate of 14.5% through the past three years. Over the past 3 years i2m grew by approximately 300% in sales of delivering cloud services solutions.

Employee retention rates

Over the last two (2) years: 100% retention rate for cloud services employees and staff and executives. We also have a 92% retention rate for all of our staff as a whole.

Who are we

For over a decade, since 2005, i2m has been a full service IT Managed Service Provider, helping companies better utilize technology to become successful and grow, helping large enterprises and public sector organizations better utilize their existing technologies and enable cloud enhancement to become more efficient and agile, helping every business become more competitive and use technology as a differentiator.

What we do

We find ourselves using cloud technologies more and more. Not because it’s “cool” right now and not because it's the "next big thing," but because we are finding that it offers access to technologies and infrastructure that our clients could never hope to reasonably build or reproduce locally. Cloud technologies offer low cost redundancy, backups and disaster recovery solutions, help control costs when extending existing, or building new, infrastructure, and offer a low barrier of entry. It's getting harder and harder for us to recommend significant investments into local infrastructure, when for a small monthly fee, we can build best-of-breed solutions in a best-of-breed cloud based environment.

From a single server or service to running your entire business on the cloud, i2m offers custom and turn-key solutions. From design and build, implementation and integration to training, management, monitoring, optimization and support once it's all running.

Why i2m?

Because we pride ourselves in being a different type of technology provider, one that is interested in your success above all else. We take our projects personally; your success is our success. We take the time to present solutions in ways you can understand, no techno-babble here. We have dedicated highly certified and trained engineers that offer an extra-ordinary level of support. Focusing on no-nonsense solutions and rapid execution, i2m is a trusted and reliable partner for companies that lack access to the broad set of resources required to design and implement complete technology solutions. We pride ourselves in efficiency by using automation and deployment tools for management, optimization and operations to further remove human error, by delivering efficiency and rapid project execution to our clients. Let i2m help guide you through the exciting options that cloud technologies can offer your company. Let us show you how surprisingly affordable a complete, managed, and monitored cloud solution from i2m can be.

Cloud Solutions Partner Qualifications

i2m is an AWS Authorized Commercial and Government Reseller, AWS Solutions Provider, Public Sector Partner and Consulting Partner. We are a part of the AWS Windows EC2 Service Delivery Program. i2m is in process for applying for AWS Storage Competency Program which recognizes AWS partners for implementing Best Practice Storage Solutions on AWS.

We have been an AWS Partner since 2013 and has been implementing Cloud Solutions since 2008 on AWS and on other public and private cloud platforms and services. We specialize in implementing AWS cloud solutions for the public and commercial sector and hold all Professional Level Certifications for AWS Services; AWS Certified Professionals and AWS Certified Associates Certifications. Electronic copies of AWS Professional and Associate Certification badges can be found in "i2m - AWS Certifications and Partner Badges.pdf" uploaded with the documents of this proposal or can be requested on-demand.

i2m has engaged in over 40 large successful cloud migration and implementation projects on AWS using the specified cloud services for over 5 years. We have engaged with projects with State and Federal Government (DOD) along with several large and small enterprises. See below (section 6.2(M)(E) SCOPE OF EXPERIENCE) for the list of case studies and projects performed by i2m for these Enterprise, State and Federal Government clients.

AWS Validated Qualifications

aws partner network

Advanced

Consulting Partner

Public Sector Channel Partner

Channel Partner

Public Sector Partner

AWS Services Delivery Badges:
Amazon EC2 for Microsoft Windows

Programs:
Authorized Commercial Reseller
Authorized Government Reseller
AWS Public Sector Partner: Government, Non-Profit

Professional Certifications:

- AWS Cloud Solutions Architect – Associate
- AWS SysOps – Associate
- AWS Developer – Associate
- AWS Cloud Solutions Architect – Professional
- AWS DevOps Engineer – Professional

Accreditations:

- AWS Technical and Business Professional Accreditation
- AWS TCO and Cloud Economics

Partner Certifications:

- AWS Windows EC2 Service Delivery Program

AWS Partner Page:

https://aws.amazon.com/partners/find/partnerdetails/?n=i2m.cloud&id=001E000000rUoGeIAK

Along with AWS we are partner and resellers of the remaining cloud services offered in this RFP. We have completed accreditations for implementing these cloud SaaS services offerings. Accreditations available on demand. We are experts in implementing these cloud services that compliment and value add to AWS (IaaS, PaaS, SaaS) services:

- Druva Partner and Reseller
- Duo Partner and Reseller
- CloudBerry Partner and Reseller
- CloudHealth Partner and Reseller
- Trend Micro Partner and Reseller

i2m Reported Qualifications

Solution Areas

Archiving
Business Applications - Microsoft
Business Applications - Other
Content Delivery
Database & Data Warehouse
Dev & Test
Disaster Recovery
High Availability
Security & Compliance
Storage (Backup, Recovery & Asset Storage
Value (Cost Savings/TCO)
Web & Web Apps

Industry Area

Business & Consumer Services

Target Client Base

Small Business
Enterprise
Government - Local
Government - National
Mid-size Business
Non-Profit
Startup

Technologies

Apache
Linux
Microsoft Exchange
Microsoft SharePoint

Microsoft SQL
MySql
PHP
System Management

Professional Services
Cloud Migration Services
Custom Application Development
Managed Service Provider
Strategic / IT Consulting
Systems Integration
Training

Assessments
US FEDERAL SOCIO-ECONOMIC STATUS
SBA Certified Small Business(SB)

6.2 (M)(E) SCOPE OF EXPERIENCE

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

Response:

Number	Name of Public Agency	Year of the Project	Contact Name	Phone Number
1	Diversified Lighting Associates	2016-2018	Trish Metzler	(215) 442-0700

Description of project #1, and what dispositions or solutions were used to benefit the customer.

Business Challenge

Diversified Lighting Associates (DLA) is a commercial lighting distributor. Prior to i2m migration, they faced the following challenges:

- Headquarters, Branch offices and remote users suffered from weather-prone infrastructure and power outages
- Slow performance of local legacy infrastructure
- Connectivity issues with branch offices caused data syncing difficulties with headquarter's applications

- Legacy client machines at branch offices were running mismatched MS Office licenses and versions
- Exchange email was hosted on a non-dedicated server, creating heavy bandwidth bottlenecks
- A legacy back-up system was prone to errors and required frequent maintenance, as well as expensive physical storage space and servers
- An on-site monitoring/alert system that often failed

i2m Solution

Recognizing that AWS would be an ideal fit for DLA, i2m implemented a plan to maximize the benefits of both, including the following changes to DLA's IT infrastructure:

- Consolidated multiple servers, including a few legacy NetWare servers, at each site into a MS Active Directory infrastructure
- Redesigned and migrated on-site infrastructure to a cloud-based Windows Active Directory infrastructure with File/Print/Application and Remote Desktop Servers, which are shared by their branch offices and remote users
- Designed to allow for high availability and redundancy
- Created ISPEC VPN tunnels to each branch office and headquarters, ensuring a secure connection between the offices and the AWS Virtual Private Cloud
- Migrated mission-critical database applications from their local Database server to the cloud, while leaving the on-site Database in place to sync with the cloud-based database server. This allowed headquarters staff to connect to the cloud-based database server reducing local load and increasing performance
- Created a new Exchange based e-mail system, giving branch offices and headquarters direct access to the email system, which reduced traffic and increased speed.
- Connected headquarters, branch offices and remote users directly to a cloud-based Remote Desktop Server using Remote Apps and full RDP desktops, allowing users to access their data and applications from anywhere, at any time
- Implemented i2mcloud Enterprise Backup (CloudBerry Managed Backup), which is a serverless back-up solution that uses AWS S3 as a back-end and light clients on each server or other critical machines that need to be recovered
- Druva In-Sync for mobile device security and backup
- Designed a reliable cloud-based monitoring and alerting system
- Use CloudHealth for Cost Management, Governance, Security, Optimization

The following AWS technology was used:

- Windows and Linux EC2
- VPC
- VPN
- Route53
- S3
- Glacier
- IAM

- Cloudtrail
- Cloudformation
- Directory Services

The following i2m.cloud technology was used:

- i2m.cloud Zimbra Exchange Email
- i2m.cloud Enterprise Backup
- i2m.cloud Monitoring/Alerting System

i2m Solution Benefits

By migrating DLA to the cloud, i2m optimized their infrastructure, which allowed remote users, branch offices, and headquarters to connect seamlessly to the cloud environment anywhere, any time, and from any device. This connectivity increased DLA's stability, availability, and redundancy, as well as increased performance gains for their critical business applications. Using Microsoft Office365 and i2m SaaS services made software compliance, deployment, and management simple and efficient. Migrating to a cloud-based infrastructure has had many benefits, including a 30% decrease in IT support calls and system problems, and quick recovery in case of failure. Full recovery time was reduced from 1-2 weeks to just a few hours.

DLA is now able to focus on their core business, rather than their IT systems and applications. These solutions did not require any up front capital cost and give DLA the scalability and flexibility to meet for their future technology needs. Migrating to the cloud also gave DLA the power to quickly adopt new technology and to test and develop new software applications and services to meet their needs.

The success of this migration pushed DLA with the help of i2m to move their headquarters infrastructure to a complete cloud-based environment, making DLA a solely cloud-based business. All systems are cloud based if not minimal hybrid architecture for legacy systems and devices. We provided more security, availability, and DR functionality using AWS Best Practice methodologies. The Goal was to create a lean Active Directory and Windows Application Server Environment that is able to scale and be agile with DLA's growth year over year.

Staff embraced the new cloud environment quickly as they required no additional training for using their applications in the cloud (very minimal access training for using RDP/Remote APPs and VPN) as they are using their applications and environment just as they were before with no perceivable difference. We had aimed to exceed performance of the existing on premise environment. DLA Stake Holders were happy with the results of the Cloud Migration and were proud to be one of the first Lighting Distribution companies running an all Cloud Native Environment that is fully managed and supported by i2m.

http://www.dlafirst.com/

2	Impact Services Corporation	2016 - 2017	Casey O'Donnell	(215) 739-1600

Description of project #2, and what dispositions or solutions were used to benefit the customer.

Business Challenge

Impact Services Corporation is a large non-profit organization with over 200 employees. Prior to their cloud migration, they faced the following challenges:

- Slow performance of local legacy infrastructure
- Connectivity issues between headquarters and branch offices
- Exchange email hosted on a non-dedicated server, creating heavy data bandwidth bottlenecks
- A legacy backup system, which experienced repeated failures and required frequent maintenance, as well as expensive local physical storage space and servers
- An unreliable monitoring/alerting system
- Slow and unreliable accounting application deployment

i2m Solution

i2m designed and implemented a plan to maximize the benefits of Amazon Web Services (AWS). The implementation included the following changes to Impact Service Corporation's IT infrastructure:

- Consolidated and migrated on-site IT infrastructure to a cloud-based Windows Active Directory infrastructure with File/Print/Application and Remote Desktop Servers, which are shared by branch offices and remote users
- Designed to allow for high availability and redundancy
- Created IPSEC VPN tunnels to each branch office, ensuring a secure connection between the offices and the AWS Virtual Private Cloud
- Migrated mission-critical accounting application, Microsoft Dynamics GP (Great Plains), from a legacy Windows 2003 MS SQL to Windows Server 2012 R2, utilizing RDS/Remote App for access
- Created a new Exchange based email system, giving branch offices and headquarters direct access to the email system, which reduced traffic and increased speed
- Connected branch offices and remote users directly to a cloud-based Remote Desktop Server using Remote Apps or full RDP desktop, which allows 24/7 access to data and applications
- Implemented i2mcloud Enterprise Backup (CloudBerry Managed Backup), which is a serverless back-up solution that uses AWS S3 as a back-end and light clients on each server or other critical machines that need to be recovered
- Druva In-Sync for mobile device security and backup
- Designed a reliable cloud-based monitoring and alerting system
- Use CloudHealth for Cost Management, Governance, Security, Optimization

The following AWS technology was used:

- Windows and Linux EC2
- VPC
- VPN
- Route53
- S3
- Glacier
- IAM
- Cloudtrail

- Cloudformation
- Directory Services

The following i2m.cloud technology was used:

- i2m.cloud Zimbra Exchange Email
- i2m.cloud Enterprise Backup
- i2m.cloud Monitoring/Alerting System

i2m Solution Benefits

Migrating to the cloud optimizes IT infrastructure, which allows headquarters, branch offices, and remote users seamless connectivity 24/7, from any device. Cloud migration increases stability, availability, and redundancy, as well as increases performance gains for critical business applications.

Impact Service Corporation users noticed immediate performance improvements with the implementation of a cloud-based Microsoft Dynamics (GP). The application was quick and stable, and users easily adapted to the new version. With the Remote App Setup, processing now occurs in the cloud, but it performs for the end user as if it is a local application.

An updated IT infrastructure allows for more efficient and effective personnel, which lowers operating expenses. Impact Services Corporation is now able to focus on serving their community. These solutions did not require any significant upfront capital expenditures, and they give Impact Services Corporation the scalability and flexibility to meet their future technology needs at a low monthly rate. Migrating to the cloud also gave them the power to quickly adopt new technology and software applications to meet their needs.

Further projects include replacing legacy workstations with Amazon Workspaces. The cloud desktops will extend the life of Impact Services Corporation's infrastructure, and convenient pay-as-you-go billing options eliminate the need for upfront capital.

http://www.impactservices.org/

3	Pennsylvania CareerLinks Philadelphia Works	2015-2018	Adrian Jezierski	(215) 557-2613

Description of project #3, and what dispositions or solutions were used to benefit the customer.

Solution Summary

i2m provides provide Full IT Support, Management and Cloud Services for these 2 Government Agencies ; 5 Pennsylvania CareerLinks and Philadelphia Mayor' Office:

Implemented as a full technology management and services solution which includes:

Data Center Virtualization, Server Maintenance and Support, Cloud Backup & Maintenance Solution, Help Desk and On-site Support (level 1-3), Network WAN/LAN management, Cloud based monitoring solution.

https://www.pacareerlink.pa.gov

6 different sites and locations throughout Philadelphia supporting and servicing approximately 1,300 clients/day

- PA CareerLink West Philadelphia
- PA CareerLink Northwest Philadelphia
- PA CareerLink North Philadelphia
- PA CareerLink Suburban Station Philadelphia
- PA CareerLink 1800 JFK Philadelphia
- PA Philadelphia Mayor's Office of Re-Entry

Solutions Benefits

Due to the success of the management and services offered to the first 3 Sites, i2m was awarded within past month with 3 additional CareerLink sites. We are currently in process of converting the 3 new sites Suburban Station, 1800 JFK, and Mayor's Office into a complete i2m solution. Making i2m the preferred solution provider for the Philadelphia region.

4	Face2Face	2018	Mary Kay	(215) 849-0179

Description of project #4, and what dispositions or solutions were used to benefit the customer.

Business Challenge

Face to Face is a not-for-profit 501(c)(3) human services organization dedicated to the health, well-being, and stability of our community. Face to Face meets basic human needs and reduces suffering. With hospitality, we provide a safe environment and practical tools, which enable the people of our community to confront personal challenges, empower their lives, and fulfill their unique potential. Prior to their cloud migration, they faced the following challenges:

- A local legacy infrastructure that was error prone with slow performance
- Connectivity issues between headquarters and branch offices
- No Remote Connectivity to local resources
- Utilizing public online email and sharing services without any management or support
- A legacy backup system, which experienced repeated failures and required frequent maintenance, as well as expensive local physical storage space
- Non- Existent Active Directory or LDAP Environment
- Shared Storage Service where files were not easily accessible and error prone
- No monitoring/alerting system in place

i2m Solution

i2m designed and implemented a plan to maximize the benefits of Amazon Web Services (AWS) and i2mcloud. The implementation included the following changes to FacetoFace's IT infrastructure:

- Consolidated and migrated on-site and public services IT infrastructure to a cloud-based Windows Active Directory infrastructure with File/Print/Application Servers, which are shared by headquarters and remote users
- Designed to allow for high availability and redundancy of Active Directory and File System
- Created IPSEC VPN tunnels to headquarters, ensuring a secure connection between the offices and the AWS Virtual Private Cloud
- Created a new MS Exchange based email system utilizing O365, giving offices and headquarters direct access to the email system, which reduced reliance on public services that were unsupported and non-industry standard
- Connected remote users directly to a cloud-based Resources and Applications which allowed 24/7 access to data and applications.
- Implemented i2mcloud Enterprise Backup (CloudBerry Managed Backup), which is a serverless back-up solution that uses AWS S3 as a back-end and light clients on each server or other critical machines that need to be recovered
- Designed a reliable cloud-based monitoring and alerting system
- Use CloudHealth for Cost Management, Governance, Security, Optimization

The following AWS technology was used:

- Windows and Linux EC2
- VPC
- VPN
- Route53
- S3
- Glacier
- IAM
- Cloudtrail
- Cloudformation
- Directory Services

i2m Solution Benefits

Migrating to the cloud optimizes IT infrastructure, which allows headquarters, offices, and remote users seamless connectivity 24/7, from any device. Cloud migration increases stability, availability, and redundancy, as well as increases performance gains for critical business applications.

Users noticed immediate performance improvements with the implementation of a cloud-based solutions for O365 and File System and sharing services.

An updated IT infrastructure allows for more efficient and effective personnel, which lowers operating expenses. Face to Face is now able to focus on serving their community and those in need. These solutions did not require any significant upfront capital expenditures, and they give Face to Face the scalability and flexibility to meet their future technology needs at a low monthly rate. Migrating to the cloud also gave them the power to quickly adopt new technology and software applications to meet their growing needs.

http://facetofacegermantown.org

5	Leggett and Platt, Inc.	2016-2018	Kiran Mungra	(425) 822-8271

Description of project #5, and what dispositions or solutions were used to benefit the customer.

Business Challenge:

Western Pneumatic Tube Company is a subsidiary of Leggett and Platt, Inc a Fortune 500 listed company, they are a manufacturing plant that produces mission critical metal tubing for the aerospace industry. Their tubing is in many of the most popular commercial airplanes that you have probably traveled in. Western Pneumatic Tube Company has an XRAY process which is used to test every nano-meter of each tube for any defects, weld points, or weakness in structure, this process is extremely technical and is meant to ensure the precision quality and safety of the products produced. This X-RAY process produces a high volume of X-Ray Images on a daily basis. These X-Ray Images must be preserved for each of their customers in case of aerospace faults, investigative purposes for a reference of history in case any unforeseen disaster may occur these X-RAY images are recalled to make sure that there was no fault in the tubing used. This required that all the X-Ray Images be archived for production to Local Storage. This was being handled by Multiple Storage NASs to provide a Primary and Secondary in case one of the physical devices fail. Which they did quite often. This legacy type of Archiving method was outdated used up too much of the local bandwidth available on the network. Users on each side of the manufacturing plant were suffering from Application/File Access performance degradation while the X-RAY Imaging Process of Archiving was carried out. IT had to constantly bring up new NAS's and replace dying ones frequently. The amount storage space was always limited, always having to add more space to suffice the substantial amount of data produced daily.

i2m Solution

We recognized the use of AWS cloud services, would be the perfect fit for this business challenge. We decided to use the AWS Snowball, to export all the existing Archived Data 10's of TB of data, along with Amazon S3 and Glacier. Data was first imported to S3 by using the AWS Snowball. Once all the data that was archived on NASs was uploaded to S3, we then archived that data into Glacier. We were then able to restore any X-RAY images required by customers or Western Pneumatic in 3-5 hours. We then created a recurring backup job using i2mcloud Enterprise Backup to fetch any new images produced daily and back that up to S3 Storage, for seldom and fast retrieval of any X-RAY images that are most recently produced.

The following AWS technology was used:

- Windows and Linux EC2
- VPC
- VPN
- Route53
- S3
- Glacier
- IAM
- Cloudtrail and AWS Config

i2m Solution Benefits

By utilizing i2m and AWS Glacier we were able to provide an infinitely scalable enterprise archiving solution that was extremely durable, redundant compared to using the on premise storage devices. All the local Archiving Storage NAS's were decommissioned. This reduced the IT dependency, time and money spent maintaining the hardware and storage infrastructure. Using the AWS Snowball made it easy, fast and secure to transfer the substantial amounts of data out of their local infrastructure into AWS. Using S3-IA along with i2mcloud Enterprise Backup to back up the most recent XRAY Images, provided a fast and easy way to retrieve any images required on the fly. This was the least expensive solution compared to other solution that were analyzed like tape and other local archiving solutions. XRAY images now are processed a lot faster more securely, and stored with higher durability. This left both the IT Staff and Western Pneumatic Staff able to sleep at night and not worry about failing or dying infrastructure that constantly need to be maintained and now has a solid, scalable and affordable archiving solution for their customers.

http://leggettaerospace.com/

6	Sharp Packaging Services	2017-2018	Mike Kegg	(610) 234-0080

Description of project #6, and what dispositions or solutions were used to benefit the customer.

i2m Solutions

-Large scale Druva In-Sync Cloud Protection Suite Implementation and Management
-Cloud Web Hosting
-Cloud based S/FTP
-Cloud based DNS Management
-Global Cloud Alerting/Monitoring Solution

http://www.sharpservices.com/

Contact Name: Mike Kegg
WorkPhone: (610) 234-0080
CellPhone: (484) 919-0668
Email: michael.kegg@sharpservices.com

7	US Federal Government (DOD) clients utilizing cloud solutions offered by i2m	2017-2018	N/A	N/A

Description of project #7

N/A

Start of Confidential
(Start of Paragraph 1)

End of Confidential
(End of Paragraph 1)

6.3 (M) FINANCIALS

Start of Confidential
(Start of Paragraph 2)

End of Confidential
(End of Paragraph 2)

6.4 (E) GENERAL INFORMATION

6.4.1

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

Response:

The depth and breadth of our solutions extend to the core offering in this proposal, AWS, which includes the all three deployment models IaaS, SaaS and PaaS. AWS is the most highly used and industry standard Public, Private and Hybrid Cloud Service Provider according to Gartner, 451 Research, Enterprise Strategy Group, Crisp Research, Kuppingercole, Monzo, Nucleus, IDC, OVUM and many other highly acclaimed reporting agencies. It is the most highly utilized, awarded and growing cloud service provider ahead of the competition Microsoft Azure and Google Cloud Platform and others in the cloud marketplace for several years now. Although we do utilize some of these other cloud service providers our core focus has been with building and designing solutions on AWS. We believe the rate and pace of innovation and breadth of services that AWS has to offer is incomparable for the foreseeable future. Here are the Gartner and other reports that back these claims: https://aws.amazon.com/resources/analyst-reports/ . AWS has also gain popularity in the portability of the majority of its services to other cloud providers or even on premise solutions. Making it easy for organizations to migrate their solutions between cloud service providers and on premise environments avoiding vendor lock in.

All SaaS services offered; DUO, Druva, CloudBerry, CloudHealth and Trend Micro are highly recognized and supported by the leader in cloud services AWS and other industry leaders in the market as well. These SaaS services have highly evolved on AWS becoming AWS Advanced Technology Partners for their excellence in implementing and running their SaaS services on AWS. These compromise the core SaaS services that we are offering in our proposal. These are cloud native and modernized SaaS solutions. All these solutions integrate between the public, hybrid and private cloud deployment models including on premise deployments. They are also portable and highly integrate with all major cloud services providers; GCP, Azure, IBM and several other service providers. They include features specific meant for several providers to give the consumer the option to choose their service provider of choice or a mix of them as their backend.

If an organization decides to move or migrate to another cloud service provider's infrastructure solution or to create a multi cloud strategy for their organizations, these IaaS, PaaS, SaaS solutions support this natively. These chosen solutions were analyzed and tested by i2m to be highly portable and integrated with existing on premise infrastructure solutions and all major cloud services providers.

6.4.2

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

Response:
i2m has auditing and reporting capabilities for SAS 70 and later versions including, SSAE 16 6/2011, SOC1, SOC2. We only have been self-audited for SOC2 similar controls by meeting controls set forth in our response in section 8.6.3 of technical proposal i2m "**i2m IT General Security Computer Controls"** "General Security Computer Controls" (GSCC). However, i2m provides compliance, auditing and controls services to meet these compliances for many of our clients. One of largest enterprises we manage on the Fortune 609 list (company name not mentioned for privacy). i2m provides full auditing and controls services for two of their large subsidiaries of their Aerospace Division. We have achieved very high compliance ratings from their corporate office over the past 5 years for assisting and maintaining their SOC1 and SOC2 audits successfully.

6.5 (E) BILLING AND PRICING PRACTICES

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

6.5.1

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

Response:
Our pricing methodology and practices are very simple it is percent of discount off manufacturer's list price or catalog. i2m supplies these cloud service with a percentage discount from the MSRP List Price. As a cloud service provider and partner we will supply the member with cloud services using these services providers and manufactures; Amazon Web Services (AWS), Druva, Duo, CloudBerry, Trend Micro and CloudHealth. Each manufacturer has a different percentage discount across their product lines specified in the Cost Proposal documents.

Amazon Web Services price list is in "AWS Price Sheets" folder, which includes in full detail each AWS service and relative price list sheet. We are providing NASPO ValuePoint and its Purchasing Entities with an i2m discount on all AWS Services at a 4.5% discount from the AWS List Price specified in the pricing catalog. Druva, Duo, CloudBerry and CloudHealth cloud services are listed in the Cost Proposal only, there is no manufacturer pricing catalog for these services. Pricing information is constantly updated with the release of new services and discounted services pulled by i2m from the Manufactures' websites, partner portals, or API endpoints. i2m does this on monthly basis to ensure it is meeting new technology and services demands rapidly and will relay these price changes or updates to its awarded contracts.

AWS Price Sheets Notes:

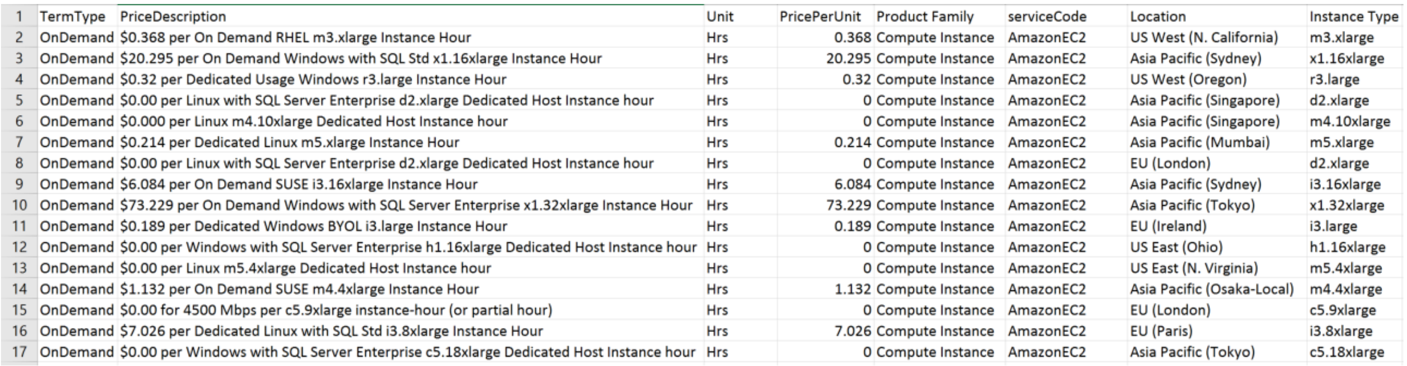
Here are some notes for reference or clarification when looking at the Pricing Sheets for AWS Services.

Please make sure to expand and sort the columns in each pricing sheet for a complete view of each service you can sort on the "PriceDescription" column for seeing like named services for example or sort to what best fits what services you're looking for.

Some Important Columns

- **TermType---PriceDescription---Unit---PricePerUnit**

- The "PricePerUnit" column is the most important column as far as pricing to determine your rates/cost for each service/line item. Each "PricePerUnit" item and its value with decimal points are carried through in calculating your monthly bill. Although the total cost of each services item on an invoice at the end of the month does not show these decimal points (e.g. $1.40 was rounded up from $1.40125) as they are rounded up to show the correct $0.00 dollar amount but the true value is what is multiplied in the formula= "Price Per Unit" column multiplied by the "Units" column consumed per month and it's quantity.



1	TermType	PriceDescription	Unit	PricePerUnit	Product Family	serviceCode	Location	Instance Type
2	OnDemand	$0.368 per On Demand RHEL m3.xlarge Instance Hour	Hrs	0.368	Compute Instance	AmazonEC2	US West (N. California)	m3.xlarge
3	OnDemand	$20.295 per On Demand Windows with SQL Std x1.16xlarge Instance Hour	Hrs	20.295	Compute Instance	AmazonEC2	Asia Pacific (Sydney)	x1.16xlarge
4	OnDemand	$0.32 per Dedicated Usage Windows r3.large Instance Hour	Hrs	0.32	Compute Instance	AmazonEC2	US West (Oregon)	r3.large
5	OnDemand	$0.00 per Linux with SQL Server Enterprise d2.xlarge Dedicated Host Instance hour	Hrs	0	Compute Instance	AmazonEC2	Asia Pacific (Singapore)	d2.xlarge
6	OnDemand	$0.000 per Linux m4.10xlarge Dedicated Host Instance hour	Hrs	0	Compute Instance	AmazonEC2	Asia Pacific (Singapore)	m4.10xlarge
7	OnDemand	$0.214 per Dedicated Linux m5.xlarge Instance Hour	Hrs	0.214	Compute Instance	AmazonEC2	Asia Pacific (Mumbai)	m5.xlarge
8	OnDemand	$0.00 per Linux with SQL Server Enterprise d2.xlarge Dedicated Host Instance hour	Hrs	0	Compute Instance	AmazonEC2	EU (London)	d2.xlarge
9	OnDemand	$6.084 per On Demand SUSE i3.16xlarge Instance Hour	Hrs	6.084	Compute Instance	AmazonEC2	Asia Pacific (Sydney)	i3.16xlarge
10	OnDemand	$73.229 per On Demand Windows with SQL Server Enterprise x1.32xlarge Instance Hour	Hrs	73.229	Compute Instance	AmazonEC2	Asia Pacific (Tokyo)	x1.32xlarge
11	OnDemand	$0.189 per Dedicated Windows BYOL i3.large Instance Hour	Hrs	0.189	Compute Instance	AmazonEC2	EU (Ireland)	i3.large
12	OnDemand	$0.00 per Windows with SQL Server Enterprise h1.16xlarge Dedicated Host Instance hour	Hrs	0	Compute Instance	AmazonEC2	US East (Ohio)	h1.16xlarge
13	OnDemand	$0.00 per Linux m5.4xlarge Dedicated Host Instance hour	Hrs	0	Compute Instance	AmazonEC2	US East (N. Virginia)	m5.4xlarge
14	OnDemand	$1.132 per On Demand SUSE m4.4xlarge Instance Hour	Hrs	1.132	Compute Instance	AmazonEC2	Asia Pacific (Osaka-Local)	m4.4xlarge
15	OnDemand	$0.00 for 4500 Mbps per c5.9xlarge instance-hour (or partial hour)	Hrs	0	Compute Instance	AmazonEC2	EU (London)	c5.9xlarge
16	OnDemand	$7.026 per Dedicated Linux with SQL Std i3.8xlarge Instance Hour	Hrs	7.026	Compute Instance	AmazonEC2	EU (Paris)	i3.8xlarge
17	OnDemand	$0.00 per Windows with SQL Server Enterprise c5.18xlarge Dedicated Host Instance hour	Hrs	0	Compute Instance	AmazonEC2	Asia Pacific (Tokyo)	c5.18xlarge

Sample AWS Pricing Sheet

Item	Price Per Unit	Unit	#Units	$per unit /Month	$per unit /Year	$monthly Total	$Yearly Total
c3.xlarge (Linux) with EBS Optimization TermType (On-Demand) Upfront Price: $0.00 Unit=Effective Hourly Cost Year calculated at 730 hours per month	$0.44567	per hour	16	$325.34	$3,904.07	$5,205.43	$62,456.11
1 GB EBS (throughput optimized)	$0.05022	per month	100000	$0.05022	$0.60	$5,022	$60,264.00

This is a pricing sheet example simplified for cost estimation
(Does not relate to pricing sheets or real pricing)

Calculated as:
The tables shows rounded numbers for all columns but actually using all decimal points throughout the calculation then rounding up to the 2 nearest decimal points at the end of the calculation.

Row 1:
$0.44567 (per hour) * 730 (hours)=325.3391 * 16 (units) =$5,205.4256 * 12 (months) = =$62,456.1072=**$62,456.11**

Row 2:
$0.05022(per unit month) * 100000 (units)= $5,022 * 12 (months) =$60,264.00000=**$60,264.00**

We added some Unit measures to be accurate with the Service Item in the list. EC2 instances rows for example have 730 hours per month to give the usage per month a baseline as this varies with real EC2 usage per different months and hours per different month. The Total $Year charge is what is expected be paid over the year.

Billing Practices:

i2m’s billing practices are also very simple and measurable similar to that of a utility bill were the billing is based on usage and consumption of services from the prior month or period of billing. Billing will follow one of these billing models; license per user/month, license per device/month or based on consumption of services IaaS, SaaS and PaaS services offered. Also rates defined for value add-on services for the period of billing.

All usage is calculated at the end of each month for AWS and is calculated automatically using our Billing and Cost management tool Cloud Health which pulls billing and usage information directly from the Cloud Services Accounts (i.e. AWS) at the end of each month or billing period. Producing a fine grained detail report of all the services usages, license usage and cost per month. There is no human intervention in our billing, unless specifically reported to NASPO ValuePoint and its Purchasing Entities for errors or credits due.

The SaaS solutions offered billing practices are the same as detailed above, either dependent on usage from prior month/billing period or amount of licenses consumed within the license term.

Month Starts at 00:00:00 hour of the first day in each month
Month Ends at 23.59:59 hour of the last day in each month

NASPO ValuePoint Purchasing Entities will be able to request at any time the detailed billing and usage reports direct from manufacturer billing consoles or from i2m. Purchasing Entities can request comparison of CSP cost to i2m proposed pricing for further verification that the Purchasing Entity is receiving the correct discount and proper usage across their monthly bills according to the NASPO ValuePoint agreement. Account review rates will apply.

6.5.2

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

Response:
There are no specific cost impacts that relate to our service offerings. The services and solutions offered inherit all the cost and pricing models of the CSPs solutions and services. The Purchasing Entity is responsible for its usage and cost that it not exceed it expectations or allotted cost/usage required by their contracts. We the Solutions provider can provide Cost Optimization services that include budget alerts and usage level alerts so that the Purchasing Entity does not exceed its expected spend or usage per month. These features can also be managed within each solutions offerings solutions (ie AWS, CloudHealth).

i2m Implementation Cost
The Purchase Entity recognizes that providing these cloud services offerings does not include implementation cost of these services. These are separate line items defined as Value-Add Services, Migration and Consulting Services in the Cost Proposal with in this

proposal. We give access to cloud services offerings accounts and initial training on accounts, accounts retrieval, general support around the contract and delivery of services. This is later clarified in throughout the proposal.

AWS Cost Impacts

AWS offers you a pay-as-you-go approach for pricing for over 100 cloud services. With AWS you pay only for the individual services you need, for as long as you use them, and without requiring long-term contracts or complex licensing. AWS pricing is similar to how you pay for utilities like water or electricity. You only pay for the services you consume, and once you stop using them, there are no additional costs or termination fees.
Pay-as-you-go

Unless you are in the business of building data centers, you have likely spent too much time and money doing just that. With AWS you no longer need to dedicate valuable resources to building costly infrastructure, including purchasing servers, software licenses or leasing facilities. With AWS you can replace large upfront expenses with lower variable costs and pay only for what you use and for as long as you need it. All AWS services are available on demand, and require no long term contracts and have no complex licensing dependencies.

Pay-as-you-go pricing allows you to easily adapt to changing business needs without overcommitting budgets and improving your responsiveness to changes. With a pay as you go model, you can adapt your business depending on need and not on forecasts, reducing the risk or overprovisioning or missing capacity.

By paying for services on an as needed basis, you can redirect your focus to innovation and invention, reducing procurement complexity and enabling your business to be fully elastic.

Pay less by using more
With AWS, you can get volume based discounts and realize important savings as your usage increases. For services such as S3 and data transfer OUT from EC2, pricing is tiered, meaning the more you use, the less you pay per GB. In addition, data transfer IN is always free of charge. As a result, as your AWS usage needs increase, you benefit from the economies of scale that allow you to increase adoption and keep costs under control.
As your organization evolves, AWS also gives you options to acquire services that help you address your business needs. For example, AWS' storage services portfolio, offers options to help you lower pricing based on how frequently you access data, and the performance you need to retrieve it. To optimize your savings, choose the right combinations of storage solutions that help you reduce costs while preserving

performance, security and durability.
Learn more about tiered pricing »

For certain services like Amazon EC2 and Amazon RDS, you can invest in reserved capacity. With Reserved Instances, you can save up to 75% over equivalent on-demand capacity. Reserved Instances are available in 3 options – All up-front (AURI), partial up-front (PURI) or no upfront payments (NURI).

When you buy Reserved Instances, the larger the upfront payment, the greater the discount. To maximize your savings, you can pay all up-front and receive the largest discount. Partial up-front RI's offer lower discounts but give you the option to spend less up front. Lastly, you can choose to spend nothing up front and receive a smaller discount, but allowing you to free up capital to spend in other projects.
By using reserved capacity, your organization can minimize risks, more predictably manage budgets, and comply with policies that require longer-term commitments.
EC2 Reserved Instances »
RDS Reserved Instances »
Reserved Instance Marketplace »

Example AWS M4.Large EC2 instance

1 Year No Upfront
vs.
ON DEMAND
$650.02/year (NURI)
32% SAVINGS

1 Year Partial Upfront
vs.
ON DEMAND
$552/year (PURI)
42% SAVINGS

1 Year All Upfront
vs.
ON DEMAND
$541/year (AURI)
43% SAVINGS

AWS BYOL

AWS support Bring Your Own License (BYOL) for a variety of services including Microsoft and RedHat.

6.5.3

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

Response:
Amazon Web Services (IaaS, PaaS, SaaS)

AWS (Amazon Web Services) meets all the five NIST essential characteristics and compliance as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  AWS provides a web console or command line interface for you to access and unilaterally provision computing and storage capabilities, developer resources and SaaS applications, as needed automatically without requiring human interaction with each service provider.

- **Broad network access**
  Capabilities are available over the network, web console and command line and can be accessed through standard mechanisms.

- **Resource pooling**
  The provider's resources are pooled to serve multiple consumers using a multi-tenant model or private cloud model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. AWS uses Regions made up of separate Availability Zones (AZs) which provide the customers the ability to specify location of provided resources at a higher level of abstraction to provide the best performance and availability (ie. US-EAST Region, US-WEST Region, US-EAST-1 AZ, etc…).

- **Rapid elasticity**
  Capabilities can be elastically provisioned and released on demand or in an automated fashion to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning appear to be unlimited and can be appropriated in any quantity at any time.

- **Measured service**
  Amazon Web Services can be configured to automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service

being utilized (e.g., computing resources, storage, processing, and bandwidth). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloudhealth(SaaS)

Cloudhealth meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Cloudhealth integrates with AWS to provide on-demand cost and billing reports, and governance actions to enable resource management and optimization.

- **Broad network access**
  Cloudhealth is accessible over a web console which can be accessed through standard mechanisms.

- **Resource pooling**
  CloudHealth inherits the resource pooling that is provided by AWS creating an environment that can scale with any organizations needs allow a an infinite amount of resources to support any organizations size and data demands

- **Rapid elasticity**
  Data that Cloudhealth collects from the consumers Amazon Web Services account can be expanded to indulge all available data or confined to collect only certain data which is applicable or requested by the consumer. There is no limit on the amount of accounts, users, reports or governance actions you are allowed to generate through Cloudhealth.

- **Measured service**
  CloudHealth helps manage and monitor resource usage on Amazon Web Services so that we can control, optimize and report on resources being utilized. Reports can be created in CloudHealth to provide transparency for both the provider and consumer of the utilized service. CloudBerry cost is easily measured as a % x of the Total of the AWS Spend per month for the Consolidated Billing accounts managed under its solution.

CloudBerry(SaaS)

Cloudberry meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Cloudberry provides a central web management console that can be used to provision on-demand storage and licenses to run different the versions of the Cloudberry backup agents.

- **Broad network access**
  Cloudberry is accessible over a web console or installed software agent which can be accessed through standard mechanisms.

- **Resource pooling**
  The provider uses AWS S3 storage to serve multiple consumers using either the multi-tenant model or the private cloud model depending on the consumer's needs, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The consumer is able to specify location of the storage at a higher level of abstraction (e.g., country, region, etc.).

- **Rapid elasticity**
  Capacity for the cloudberry licenses and backup storage can be provisioned and released on demand or automatically based on usage activity or consumer demand. Capabilities for provisioning storage and licenses appear unlimited and can be appropriated in any quantity at any time.

- **Measured service**
  Provisioned licenses and storage usage is monitored and controlled by i2m. Reports are generated providing transparency on license and storage usage and costs for both the provider and consumer of the utilized service.

Druva(SaaS)

Druva meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Druva backup agent's licenses and storage can be provisioned on-demand through a central Druva web management console without requiring human interaction with the service provider.

- **Broad network access**
  Druva is accessible over a web console or installed software agent which can be accessed through standard mechanisms.

- **Resource pooling**
  Druva uses AWS S3 storage to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer is able to specify location of storage at a higher level of abstraction (e.g., country, region, etc.).

- **Rapid elasticity**
  Storage capacity and user licenses are monitored for resource usage and can be provisioned and released on-demand or automatically based on usage activity. Capabilities for provisioning storage and licenses appear unlimited and can be appropriated in any quantity at any time.

- **Measured service**
  Provisioned license, active users, and storage resource usage is monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service and resources.

DUO(SaaS)

DUO meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Duo provides an admin portal which controls all additions deletions and management of user accounts which can be executed on-demand with no limitation on quantity.
- **Broad network access**
  Devices and Users can access this service globally using strategically secured placed endpoints. The Service can be accessed from web browsers, mobile clients and DUO hardware client devices.
- **Resource pooling**
  The pooling of resources to support the SaaS solution are managed by the CSP and its backend cloud provider.
- **Rapid elasticity**
  You rapidly scale the use of the SaaS service solutions on demand without any limitations to user accounts or devices managed. Users Accounts can be added removed elastically to scale usage and cost with the organizations needs.
- **Measured service**
  This is a measured service at the end of each month the user licenses are counted and reported by the CSP and Solution Provider i2m.

Trend Micro(SaaS)

Trend Micro meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Trend Micro agent licenses can be provisioned on demand without requiring human interaction with the service provider.

- **Broad network access**
  Trend Micro is accessible over a web console or installed software agent which can be accessed through standard mechanisms.

- **Resource pooling**
  Trend Micro provisioned licenses can serve multiple consumers being dynamically assigned and reassigned according to consumer demand and active user count. The customer generally has no control or knowledge over the exact location of the provided resources.

- **Rapid elasticity**
  Trend Micro licenses can be provisioned and released on-demand to scale rapidly outward and inward based consumer demand or usage activity. Trend Micro licenses can be appropriated in any quantity at any time.

- **Measured service**
  Trend Micro automatically controls licenses by basing usage on the number of active users' and not the provisioned license count which helps optimize costs. Resources usage is monitored and controlled by i2m and reports are generated to provide transparency for both the provider and the consumer of the utilized service.

6.6 (E) BEST PRACTICES

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

Response:

i2m has policies and procedures in place for cloud services management

Visibility

i2m ensures visibility into our solutions by giving full control over the Root Accounts for each IaaS, SaaS, PaaS service provided if requested. Clients can see their cost usage directly via the cloud services solution interface/APIs or through 3rd party solutions. i2m just needs to create restricted user accounts in the solution provided that are required for usage and billing purposes only. i2m does not limit the access to the solutions provided required by any organization giving limitless and untethered access to all the services, solutions and their features. We provide full visibility to service usage and consumption.

The Purchasing Entity elects the level of access and control that us, the solution provider, has protecting any sensitive workloads or data accordingly. All the solutions offered provide strict and fine detail access and authorization controls to prevent any un-authorized access which can easily be audited natively within the service or with the use of common integrations with these solutions. In some cases the Purchasing Entity may want no access by us, the solution provider, and wish to manage their accounts on their own. The Purchasing Entity may also ask i2m to implement or help implement some of their own security measures.

i2m is proposing the CloudHealth platform meant for Security, Governance, Cloud Control, Cost and Usage Management. It grants unlimited IT Admins and Financial Officers user access to the CloudHealth SaaS platform. CloudHealth is meant for creating meaningful perspectives into the AWS and SaaS environments proposed. CloudHealth has a great number of built in reports and tools to analyze spend and usage across multiple accounts and also at a Consolidated Billing Level. CloudHealth abstracts from the real Consolidated Billing Account and can split accounts' usage billing and analytics into multiple Consolidated Billing Accounts for Cost Center or departmental cost and usage segregation. i2m can provide consultation on using CloudHealth with direct access to i2m and CloudHealth Engineers we can setup several useful custom reports and perspectives into your environment.

Compliance

All of the elected cloud services solution have compliance and audit trails built into the service which will monitor and report on all API calls and changes made by users within the account. Keeping a trail of every action taken by every user. AWS uses CloudTrail, AWS Config and Guard Duty and other compliance and checking services that help organizations meet compliance. AWS also has quick start infrastructure templates that help maintain a baseline of compliance. i2m can also recommend tools outside the scope of this proposal to ensure compliances in the different federal and state organizations. All CSPs have had an audit compliance of their solutions and also hold industry standard compliance mentioned in detail in the technical sections of this proposal. More about compliance can be found in the Technical Response section of this proposal.

Data Security

All services we are offering have Industry Standard and exceeds encryption and identify services. Encrypting traffic to encrypting data at rest and during transfer. Protecting access and controls to data and resources. Encryption of all services offered meet best industry standards encryption and information security servicers. Key Management solutions and FIPS certified services like Druva and AWS. To DUO compliance with NIST, CJIS and several others. More security details found in the Technical Response section of this proposal.

Security Considerations

AWS Account Security Features

- Secure IT Access, All IT staff require MFA and username password (strict password policy) combo to do any work in any AWS Account.
- IAM (Identity and Access Management) has security features designed to give users least privileged access to services and user account management defined and secured by i2m.
- Any modification to AWS Resources or Configuration changes are tracked per i2m AWS Engineer/Architect (AWS Cloud Trail, AWS Config, AWS GuardDuty)
- Root AWS Account locked by MFA (kept in secret) and very strict password policy. These Root Account credentials are to be held by executive IT Admins or Executive Staff, only requested by i2m if needed.
- AWS also has many Encryption and Tokenization services natively built in to protect data and access to that data.

CloudHealth

- SSO with your own identity provider (IDP) (e.g. ADFS) public identity services and (IDPS)).
- Encryption of tenant information
- Secure Account access Protocols
- SSL secured web/mobile access
- Audit Trail

DUO

- SSO with your own identity provider (IDP)
- Multi Factor Authentication
- Encryption of data and rest and in transit
- SSL secured web/mobile access
- Audit trail

CloudBerry

- SSO with AD Integration

- Encryption of data at rest and in transit
- SSL secured web access
- Audit Trail

Trend Micro

- SSO with LDAP and AD integration
- SSL secured web access
- Audit Trail

Threat Protection

All of the solutions offered in this proposal have built in threat detections services that fall under a shared security responsibility model. In which the entity is ultimately responsible for maintaining security of the solutions it uses, and the CSPs protecting the underlying Infrastructure or service backend it runs on, where built in protection services and features can be used with these cloud solutions. The solution provider can implement these threat detection services and help organizations meet security requirements and compliances at will of the participating entities.

AWS includes Audit logs that provide a wealth of information on the operations, governance, and security of your AWS resources. As the complexity of workloads increases, so does the volume of audit logs being generated. Amazon GuardDuty makes it easy for organizations to analyze AWS CloudTrail logs to identify potential account and workload threats without a significant investment of time and resources.

Together, AWS CloudTrail and Amazon GuardDuty make it easier to stop potential threats using the detailed CloudTrail log files and the power of GuardDuty threat detection. Amazon GuardDuty has recently enhanced its AWS CloudTrail log analysis thereby reducing the cost to customers.

i2m can provide threat protection services for the solutions offerings in this proposal

- Daily Monitoring, Alerting, and assisted resolution
- Backup failure and error assisted resolution
- Risk Management and Consistency Checking
- Periodic Penetration Testing Services
- Periodic Security Review services
- Periodic up to the minute, Daily, Weekly, Monthly auditing, reporting and notification of the cloud solution threats and security alerts
- Central Management Consoles for audit trails, security, identity and access management
- Self-Service Portals for IT and authorized Staff

- Recommend 3rd Party Security and Threat Detection/Protection solutions the supplement the built in security services in IaaS, PaaS, SaaS solutions offered

NASPO VALUEPOINT

Organization and Staffing 7
Utah Solicitation Number SK18008
Cloud Solutions

July 6th, 2018, 3:00 PM

Include Information Management, Inc.
DBA
(i2m)

600 West Germantown Pike, Suite 400, Plymouth Meeting, PA 19462

Organization and Staffing 7

General Information			
RFP Title and Number	RFP Manager	RFP Lead	RFP Contact
Cloud Solutions SK18008 NASPO ValuePoint	Ahmed Attalla ahmeda@i2m.cloud (267) 240-9097	Solomon Kingston, State Contract Analyst State of Utah, Division of Purchasing	Solomon Kingston skingston@utah.gov (801) 538-3228

Document Preparation Information		
Primary Author	Date	Organization Name
Steven Grzywinski	June 1st , 2018	i2m i2m.cloud Include Information Management Inc.
Phone Number	E-mail	Attached Work Order / Invoice
484-433-7136	steveg@i2m.solutions	n/a

i2m Lead Team Members			
Name	Role and Organization	E-mail	Phone Number
Ahmed Attalla (Primary)	President, i2m.cloud	ahmeda@i2m.cloud	267-240-9097
Scott Miller	COO, i2m	scottm@i2m.solutions	484-238-4118
Steven Grzywinski	President and CTO, i2m	steveg@i2m.solutions	484-433-7136
Chris Messina	Senior Enterprise Solutions Architect, i2m	chrism@i2m.solutions	610-996-9622
Daniel Perez	Senior Cloud Solutions Architect, i2m.cloud	danp@i2m.cloud	209-559-5428
i2m Main Number and Fax	Support Email	support@i2m.cloud	888-991-3814

Company Information	
Years in Business	Since 2005, approximately 12 years
Ownership	Private
DUNS	033157379

7 ORGANIZATION AND STAFFING

7.1 (ME) CONTRACT MANAGER

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

7.1.1

Provide the name, phone number, email address, and work hours of the person who will act as contract manager if you are awarded a master agreement.

Response:
Contract Manager
Name: Ahmed Attalla
Title: President and CTO i2m.cloud
i2m
i2m.cloud
Include Information Management, Inc.
Direct Phone Number: 267-240-9097
Email: ahmeda@i2m.cloud
Work Hours: Monday through Friday 7 AM – 9 PM EST,
Off Hours and Weekends (Saturday-Sunday) available on-demand for emergencies, critical issues with production, cyber security and Disaster Recovery.

7.1.2

Describe in detail the contract manager's experience managing contracts of similar size and scope to the one that will be awarded from this rfp. Provide a detailed resume for the contract manager.

Response:
Contract Manager Experience
Ahmed Attalla the president of our cloud division will be the primary contract manager for NASPO ValuePoint Master Agreement. Ahmed has extensive experience in composing, managing and delivering cloud solutions for our large i2m Commercial, Federal, State and City contracts. Ahmed and the i2m team have been awarded several contracts over the past 4 years through his leadership. Ahmed is the primary contract manager to one of the largest and most import federal contracts specific i2m maintains. Along with leading our Public Sector team in delivering solutions specific to the Public Sector. He has led meeting all the

requirements from our core CSP; AWS, to become a Public Sector Partner, Reseller and Solution Provider.

With extensive experience in Cloud Solution Delivery and Project Management, Ahmed holds the highest technical rank in delivering AWS solutions obtaining all 5 Technical Professional Certifications and Business Level Accreditation from AWS. He also holds several accreditations and technical experience for implementing the SaaS Solutions offered in this proposal.

The Contract Manager also has the proper clearance and business perspective to asses and determine contract viability for i2m's scope of experience, without engaging in a contract that may put the State, City, Federal Government or its resources, assets and clients at risk. Ahmed is keen on delivering solutions that will help these agencies without sacrificing risk, security and compliance that need to be met by these agencies.

Resume

Education:

- Temple University, College of Engineering
- Bachelor of Science: Computer and Electrical Engineering 2007 – 2011
- Minored in Computer Science
- Societies: Eta Kappa Nu, IEEE
- Dean's List 2008-2011, Senior Design Project 1st place award, School of Electrical and Computer Engineering

Professional Certifications:

- AWS Cloud Solutions Architect – Associate
- AWS SysOps – Associate
- AWS Developer – Associate
- AWS Cloud Solutions Architect – Professional
- AWS DevOps Engineer – Professional

Business Accreditations:

- AWS Technical and Business Professional Accreditation
- AWS TCO and Cloud Economics
- Cloud Business and MSP Trainings

Cloud Services Experience:

- Infrastructure as a Service (IaaS) Management and Delivery
- Managed Windows Active Directory in the Cloud
- Microsoft Workloads and Applications
- Remote App and Remote Desktop Services on AWS

- Managed Cloud Desktops (DaaS)
- Software as a Service (SaaS)
- Disaster Recovery (DRaaS)
- Enterprise Class Cloud Backup and Recovery Services
- Cloud Migration and Optimization Services
- Cloud Governance, Security, Reporting and Analytics Services
- High Availability and Fault Tolerant Design and Build Services
- DevOps/SysOps Services
- Public Sector Cloud Services for Cities, States, Governments, and Non-Profits
- Cloud Authentication and Authorization Services (SSO)
- Project Management and General Technology Consulting
- Experienced Infrastructure: AWS, GTP, Azure, Softlayer XenCenter, VMware.
- Experienced Cisco Networking, IOS Configuration, Switching and Security
- Experienced with Network protocols and standards

7.1.3

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

Response:
Roles and responsibilities of the contract manager

- Primary contact for all matters concerning the NASPO ValuePoint Master Agreement
- Primary contact for all negations concerning the NASPO ValuePoint Master Agreement and Contracts resulting
- Primary Emergency, Security and Cyber Security Response Person
- Responsible for accounting, audit, contract administration, escalation, main participant contact, open order/status report, and reconciliation
- Primary pricing information officer submitting new and updated services catalogs' for the solutions offered and their pricing to NASPO ValuePoint Master Agreement and participating entities.
- Delegates contract tasks and information to i2m Project Managers, stake holders and is the lead administrative, financial and technical verification officer for all contracts and their projects
- Primary contact for performance review ensuring all contracts and their projects meet or exceed the participating entities expectations. Quality Assurance of Service Delivery and Implementation of contracts.

Additional Contact Information

Main NASPO ValuePoint representative contact: Ahmed Attalla
(Shall be the main point of contact for members and be responsible for member information requests)
Title President of i2m.cloud Email address ahmeda@i2m.cloud

Phone number 267-240-9097 Fax 888.991.3814

Contract Administrator contact: Ahmed Attalla
(Shall be the main point of contact for contract information requests.)

Title President of i2m.cloud Email address ahmeda@i2m.cloud

Phone number 267-240-9097 Fax 888.991.3814

Additional Accounting contact: Steven Grzywinski
(Shall be the main point of contact for accounting issues.)

Title President/CTO of i2m Email address steveg@i2m.solutions

Phone number 484-433-7136 Fax 888.991.3814

Open Order/Status Report contact: Ahmed Attalla
(Shall be the main point of contact regarding open orders and status reports.)

Title President of i2m.cloud Email address ahmeda@i2m.cloud

Phone number 267-240-9097 Fax 888.991.3814

Additional Audit contact: Steven Grzywinski
(Shall be the main point of contact for audit requests and clarifications.)

Title President/CTO of i2m Email address steveg@i2m.solutions

Phone number 484-433-7136 Fax 888.991.3814

Additional Reconciliation contact: Steven Grzywinski
(Shall be the main point of contact for reconciliation report requests and/or clarifications and payment of administration fees.)

Title President/CTO of i2m Email address steveg@i2m.solutions

Phone number 484-433-7136 Fax 888.991.3814

Additional Escalation contact: Scott Miller
(Shall be the main point of contact when an issue needs to be escalated above the main contact and/or contract administrator for the RFP/contract)

Title COO Email address scottm@i2m.solutions

Phone number 484-238-4118 Fax 888.991.3814

Marketing contact: Ahmed Attalla
(Shall be the main point of contact for providing marketing information for NASPO ValuePoint's website.)

Title President of i2m.cloud Email address ahmeda@i2m.cloud

Phone number 267-240-9097 Fax 888.991.3814

NASPO VALUEPOINT

Technical Response 8
Utah Solicitation Number SK18008
Cloud Solutions

July 6th, 2018, 3:00 PM

Include Information Management, Inc.
DBA
(i2m)

600 West Germantown Pike, Suite 400, Plymouth Meeting, PA 19462

8 Technical Response

General Information			
RFP Title and Number	RFP Manager	RFP Lead	RFP Contact
Cloud Solutions SK18008 NASPO ValuePoint	Ahmed Attalla ahmeda@i2m.cloud (267) 240-9097	Solomon Kingston, State Contract Analyst State of Utah, Division of Purchasing	Solomon Kingston skingston@utah.gov (801) 538-3228

Document Preparation Information		
Primary Author	Date	Organization Name
Ahmed Attalla Secondary Author: Daniel Perez Tertiary Author: Steven Grzywinski	June 1st , 2018	i2m i2m.cloud Include Information Management Inc.
Phone Number	E-mail	Attached Work Order / Invoice
267-240-9097	ahmeda@i2m.cloud	n/a

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.

Response:

Amazon Web Services

AWS (Amazon Web Services) meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  AWS provides a web console or command line interface for you to access and unilaterally provision computing and storage capabilities, developer resources and SaaS applications, as needed automatically without requiring human interaction with each service provider.

- **Broad network access**
  Capabilities are available over the network, web console and command line and can be accessed through standard mechanisms.

- **Resource pooling**
  The provider's resources are pooled to serve multiple consumers using a multi-tenant model or private cloud model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. AWS uses Regions made up of separate Availability Zones (AZs) which provide the customers the ability to specify location of provided resources at a higher level of abstraction to provide the best performance and availability (ie. US-EAST Region, US-WEST Region, US-EAST-1 AZ, etc…).

- **Rapid elasticity**
  Capabilities can be elastically provisioned and released on demand or in an automated fashion to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning appear to be unlimited and can be appropriated in any quantity at any time.

- **Measured service**
  Amazon Web Services can be configured to automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service being utilized (e.g., computing resources, storage, processing, and bandwidth). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

CloudHealth

CloudHealth meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**

CloudHealth integrates with AWS, GCP, Azure and Local Data centers or Colocation to provide on-demand cost, usage, billing reports, and automated governance actions to enable resource management and optimization without human intervention or alert and resolve for services that fall out of compliance. Where admins can integrate into these CSPs and their Local Infrastructure on the fly and data collection, alerting and remediation begin immediately.

- **Broad network access**
  CloudHealth is accessible over a web console which can be accessed through standard mechanisms via web browsers and mobile clients.

- **Resource pooling**
  CloudHealth inherits the resource pooling characteristic that is provided by AWS as its main infrastructure cloud services provider creating an environment for the SaaS solution that can scale with any organizations needs allow an infinite amount of resources to support any organizations size and data demands for the solution.

- **Rapid elasticity**
  Data that CloudHealth collects from the consumers Amazon Web Services account can be expanded to indulge all available data or confined to collect only certain data which is applicable or requested by the consumer. There is no limit on the amount of accounts, users, reports or governance actions you are allowed to generate through CloudHealth. The Service simple scales up and down with consumer demand

- **Measured service**
  CloudHealth helps manage and monitor resource usage on Amazon Web Services so that we can control, optimize and report on resources being utilized. Reports can be created in CloudHealth to provide transparency for both the provider and consumer of the utilized service.

CloudBerry

CloudBerry meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Cloudberry provides a central web management console that can be used to provision on-demand storage and licenses to run different the versions of the CloudBerry backup agents.

- **Broad network access**
  CloudBerry is accessible over a web console or installed software agent which can be

accessed through standard mechanisms.

- **Resource pooling**
  The provider uses AWS S3 storage or provider of choice for object storage to serve multiple consumers using either the multi-tenant model or the private cloud model depending on the consumer's needs, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The consumer is able to specify location of the storage at a higher level of abstraction (e.g., country, region, etc.).

- **Rapid elasticity**
  Capacity for the cloudberry licenses and backup storage can be provisioned and released on demand or automatically based on usage activity or consumer demand. Capabilities for provisioning storage and licenses appear unlimited and can be appropriated in any quantity at any time.

- **Measured service**
  Provisioned licenses and storage usage is monitored and controlled by i2m. Reports are generated providing transparency on license and storage usage and costs for both the provider and consumer of the utilized service.

Druva

Druva meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Druva backup agent's licenses and storage can be provisioned on-demand through a central Druva web management console without requiring human interaction with the service provider.

- **Broad network access**
  Druva is accessible over a web console or installed software agent which can be accessed through standard mechanisms.

- **Resource pooling**
  Druva uses AWS S3 storage to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer is able to specify location of storage at a higher level of abstraction (e.g., country, region, etc.).

- **Rapid elasticity**

Storage capacity and user licenses are monitored for resource usage and can be provisioned and released on-demand or automatically based on usage activity. Capabilities for provisioning storage and licenses appear unlimited and can be appropriated in any quantity at any time.

- **Measured service**
  Provisioned license, active users, and storage resource usage is monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service and resources.

DUO

DUO meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**
  Duo provides an admin portal which controls all additions deletions and management of user accounts which can be executed on-demand with no limitation on quantity.

- **Broad network access**
  Devices and Users can access this service globally using strategically secured placed endpoints. The Service can be accessed from web browsers, mobile clients and DUO hardware client devices.

- **Resource pooling**
  The pooling of resources to support the SaaS solution are managed by the CSP and its backend cloud provider.

- **Rapid elasticity**
  You rapidly scale the use of the SaaS service solutions on demand without any limitations to user accounts or devices managed. Users Accounts can be added removed elastically to scale usage and cost with the organization's needs.

- **Measured service**
  This is a measured service at the end of each month the user licenses are counted and reported by the CSP and Solution Provider i2m.

Trend Micro

Trend Micro meets all the five NIST essential characteristics as outlined in the NIST Special Publication 800-145.

- **On-demand self-service**

Trend Micro agent licenses can be provisioned on demand without requiring human interaction with the service provider.

- **Broad network access**
  Trend Micro is accessible over a web console or installed software agent which can be accessed through standard mechanisms.

- **Resource pooling**
  Trend Micro provisioned licenses can serve multiple consumers being dynamically assigned and reassigned according to consumer demand and active user count. The customer generally has no control or knowledge over the exact location of the provided resources.

- **Rapid elasticity**
  Trend Micro licenses can be provisioned and released on-demand to scale rapidly outward and inward based consumer demand or usage activity. Trend Micro licenses can be appropriated in any quantity at any time.

- **Measured service**
  Trend Micro automatically controls licenses by basing usage on the number of active users' and not the provisioned license count which helps optimize costs. Resources usage is monitored and controlled by i2m and reports are generated to provide transparency for both the provider and the consumer of the utilized service.

8.1.2

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

Response:
i2m complies that if it is awarded a contract under this RFP, the services offered by i2m will comply with all the requirements outlined in Attachments C & D discussed in this proposal.

8.1.3

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

Response:

Amazon Web Services

Amazon Web Services offers a wide range of services which fall under all three service models

(SaaS, IaaS, and PaaS) and aligns with the three NIST definitions for each service model. Amazon Web Services provides cloud based services through the Public, Private and Hybrid cloud deployment models.

- **Infrastructure as a Service (IaaS)**
  AWS IaaS services enable 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 limited control of select networking components (e.g., host firewalls).

- **Platform as a Service (PaaS)**
  AWS PaaS services provide the customer the capability 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.

- **Software as a Service (SaaS)**
  AWS SaaS services provide the capability to the consumer to use the provider's applications running on a cloud infrastructure through a wide range of interfaces including web browser, command line, program interfaces, and more. 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. AWS has the ability to provide cloud based services through the various deployment methods including Private Cloud, Public Cloud and Hybrid Cloud.

- **Private Cloud**
  Amazon Web Services account(s) are provisioned by i2m for the exclusive use by a single organization which may comprise of multiple consumers depending on their specific needs. i2m may also take over management of an existing consumers' Amazon Web Services account to be utilized in the same fashion. The consumer can choose whether the account is to be managed by i2m, the organization, by a third party or some combination of them. Amazon Web Services accounts and resources are hosted in AWS Regions made up of separate Availability Zones (AZs) which provide the consumers the ability to specify location of the AWS accounts at a higher

level of abstraction to provide the best performance and availability (ie. US-EAST Region, US-WEST Region, US-EAST-1 AZ, etc…). Dedicated networks, hosts, storage, connections, and other dedicated cloud resources can be utilized to adhere to the Private Cloud deployment model. (ie Dedicated hosts, Dedicated instances)

- **Public Cloud**
  Amazon Web Services account(s) are provisioned by i2m for the exclusive use by a single organization which may comprise of multiple consumers depending on their specific needs. i2m may also take over management of an existing consumers' Amazon Web Services account to be utilized in the same fashion. The consumer can choose whether the account is to be managed by i2m, the organization, by a third party or some combination of them. Amazon Web Services accounts and resources are hosted off premise in AWS Regions made up of separate Availability Zones (AZs) which provide the consumers the ability to specify location of the AWS accounts at a higher level of abstraction to provide the best performance and availability (ie. US-EAST Region, US-WEST Region, US-EAST-1 AZ, etc…). The organizations cloud resources can be configured to extend capabilities to the general public or other third parties. By default, most Amazon Web Services resources utilize shared hosts, compute capacity, storage, bandwidth and others cloud resources that are shared but logically isolated which allow it to fall under NIST Public Cloud deployment model.

- **Hybrid Cloud**
  Amazon Web Services account(s) are provisioned by i2m for the exclusive use by a single organization which may comprise of multiple consumers depending on their specific needs. i2m may also take over management of an existing consumers' Amazon Web Services account to be utilized in the same fashion. The consumer can choose whether the account is to be managed by i2m, the organization, by a third party or some combination of them. Amazon Web Services accounts and resources are hosted off premise in AWS Regions made up of separate Availability Zones (AZs) which provide the consumers the ability to specify location of the AWS accounts at a higher level of abstraction to provide the best performance and availability (ie. US-EAST Region, US-WEST Region, US-EAST-1 AZ, etc…). The organizations cloud resources can be configured to extend capabilities to the general public or other third parties. By default, most Amazon Web Services resources utilize shared hosts, compute capacity, storage, bandwidth and others cloud resources that are shared but logically isolated which allow it to fall under the NIST Public Cloud deployment model. Dedicated networks, hosts, storage, connections, and other dedicated cloud resources can also be utilized to adhere to the NIST Private Cloud deployment model. A combination of the two models can be also be utilized.

For more detailed information on how Amazon Web Services complies with NIST requirements, visit this website: https://aws.amazon.com/compliance/nist/

Community Cloud
AWS Supports Community Cloud deployment models as defined by NIST

- **Low/Moderate/High Risk Data**
  AWS can host the following data types within its infrastructure it is up to the Purchasing Entity managing this infrastructure and the services used on AWS to meet their own Compliance and Regulations. i2m can assist the Purchasing Entity with implementation of security and encryption services that apply to the data risk types below. Where AWS provides encryption services at rest and transfer where the entity can self-manage keys for any High Risk Data or use their FIPS compliance tools and features to adhere to FIPS compliance where details on AWS FIPS Compliance is referenced using the link below:

  AWS is capable of storing and securing data at all three risk levels as defined by FIPS PUB 199 (Low Risk Data, Moderate Risk Data, High Risk Data). The US East and US West regions hold a Provisional Authorization for level 2 which permits mission owners to deploy public, unclassified information in these regions with both the AWS Authorization and the mission application's ATO. The AWS GovCloud (US) region now holds a Provisional Authorization for levels 2 and 4 and permits mission owners to deploy the full range of controlled, unclassified information categories covered by these levels.

  For more detailed information on how Amazon Web Services complies with FIPS requirements, visit this website: https://aws.amazon.com/compliance/fips/

Cloudhealth

- Software as a Service (SaaS)
- Public Cloud

Cloudberry

- Software as a Service (SaaS)
- Public Cloud
- Private Cloud
- Hybrid Cloud

Druva

- Software as a Service (SaaS)
- Public Cloud

- Private Cloud
- Hybrid Cloud

DUO

- Software as a Service (SaaS)
- Public Cloud

Trend Micro

- Software as a Service (SaaS)
- Public Cloud

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.

Response:
i2m intends to provide all cloud solutions directly without the use of any subcontractors.

8.2.2

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

Response:
i2m intends to provide all cloud solutions directly without the use of any subcontractors.

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.

Response:
i2m intends to provide all cloud solutions directly without the use of any subcontractors.

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.

Start of Confidential
(Start of Paragraph 3)

End of Confidential
(End of Paragraph 3)

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.

Response:
i2m will not engage and does not permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement. i2m will contact Participating Entity or the Master Agreement before any of these activities take place to make sure if any activities do not adhere or are not warranted by the Participating Entity or the Master Agreement.

8.3.3

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

Response:

Amazon Web Services (IaaS, PaaS, SaaS)

Running development and test workloads on Amazon Web Services enables you to remove hardware-based resource constraints to quickly create developer environments and expand your testing machine fleet. You get instant access to machines that you can configure any way you want and you only pay for what you use. This agility enables you to bring new developers on faster, try out configuration changes in parallel, and run as large a test pass as you like; all with the click of a mouse. All the services within AWS ecosystem can be run in a testing/staging environment in some cases services can be run locally on a user's machine or within their local environment without incurring any costs for staging/testing. AWS has many built in features that support a CI/CD pipelines for you applications and infrastructure where the testing/staging environment can be built on your behalf along with the Production environment through use of templates and Quick Start Guides. AWS provides multiple methods of isolation and fine grained control of AWS resources and accounts that allow you to clearer identify and isolate your test/staging/qa/dev and sandbox accounts or logical segmentation between these environments within the same account.

SaaS solutions offered (DUO, Druva, Trend Micro, CloudHealth, CloudBerry):

All of these solutions support being run and integrated into any test/staging environment that is identical to production. These solutions do not require a production environment to operate on. Rather these solution can be verified and tested before use into production for POC or other application testing scenarios. Trend Micro, CloudHealth etc. offer on-demand evaluation environments please see section 8.17(E) Trial And Testing Periods for further details.

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.

Response:

i2m confirms and attests 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.

The Voluntary Product Accessibility Template (VPAT) is available to customers using AWS Artifact, a self-service portal for on-demand access to AWSs compliance reports.

AWS provides API-based cloud computing services with multiple interfaces to those services, including SDKs, IDE Toolkits, and Command Line Tools or developing and managing AWS resources. AWS provides two graphical user interfaces, the AWS Management Console and the AWS ElasticWolf Client Console. The AWS ElasticWolf Client Console has incorporated Section 508 requirements and AWS has prepared a Voluntary Product Accessibility Template (VPAT) for the Console, which outlines the Consoles accessibility features.

8.3.5

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

Response:
i2m confirms and attests its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (Internet Explorer, Firefox, Chrome, and Safari) at a minimum. This applies to AWS and the rest of the SaaS solution offerings mentioned in this RFP.

Browser	Version
Google Chrome	Latest three versions
Mozilla Firefox	Latest three versions
Microsoft Edge	Latest three versions
Apple Safari for macOS	Latest two versions
Microsoft Internet Explorer	11

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.

Response:
Prior to the execution of a Service Level Agreement, i2m is required to 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 i2m that is subject to any law, rule or regulation providing for specific compliance obligations. i2m and the Purchasing Entity must record the details of this meeting in electronic format or if required by the Purchasing Entity

to sign a secured electronic document specifying the details of the meeting and the details of the data being stored prior to the execution of an SLA. This is to formulate a plan to meet or exceed any law, rule or regulation providing for specific compliance obligations to that data.

NASPO ValuePoint Purchasing Entities and i2m should send any details about sensitive and personal information meetings by emailing support@i2m.cloud. So that there is a record of the meeting to meet the requirements. If the nature of the data need to be transmitted in more secure method we can provide you with links to our secure data store (similar to drop-box but privately managed) or other secure document transfer methods specified by the Purchasing Entity.

Email should have subject line "NASPO ValuePoint – Sensitive Information Details – The Members Legal Business Name – Project/Contract Name"

In the body of the request please include in detail the nature of your request, as specified above and a primary point of contact.

i2m will respond to the email to either schedule a meeting to further discuss, answer the details of the request or reply to the request directly via email. Virtual/Audio Conference details will be sent to the Purchasing Entity if meeting is requested. It is encouraged that the Purchasing Entity include in the meeting any relevant staff members that will be delivering/implementing the requested cloud solution to the organization.

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.

Response:
Standard delivery time for accounts for the products/services offered after receipt of purchase order
Standard Delivery time is 24-72 hours after receipt of purchase order. Some large substantial requests may take longer. The assigned Project Manager or Account Manager will provide the member an estimated time for service delivery when products/services are requested. This is just to give the Purchasing Entity the immediate access to the IaaS, SaaS, PaaS solutions accounts' specified in this RFP. The Purchasing Entities can start using services at will if this does not involve i2m implementation or value-add services. If the solution does involve implementation by i2m, i2m will inform the client what measures to take and account for, before using their cloud services accounts so it does not get in the way of any project to be implemented by i2m.

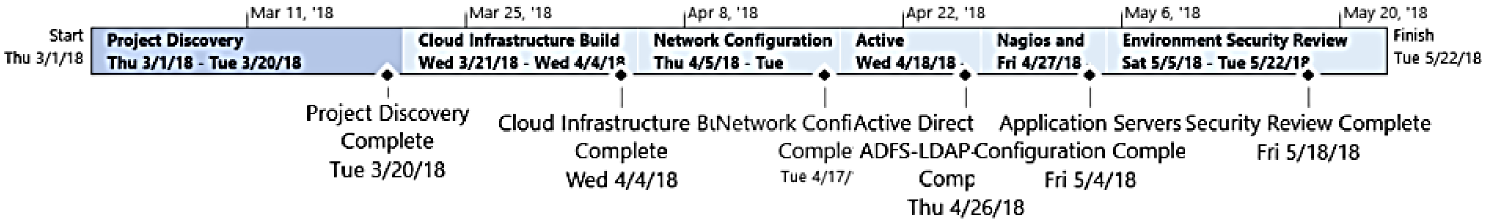
Project/Work scheduled plans

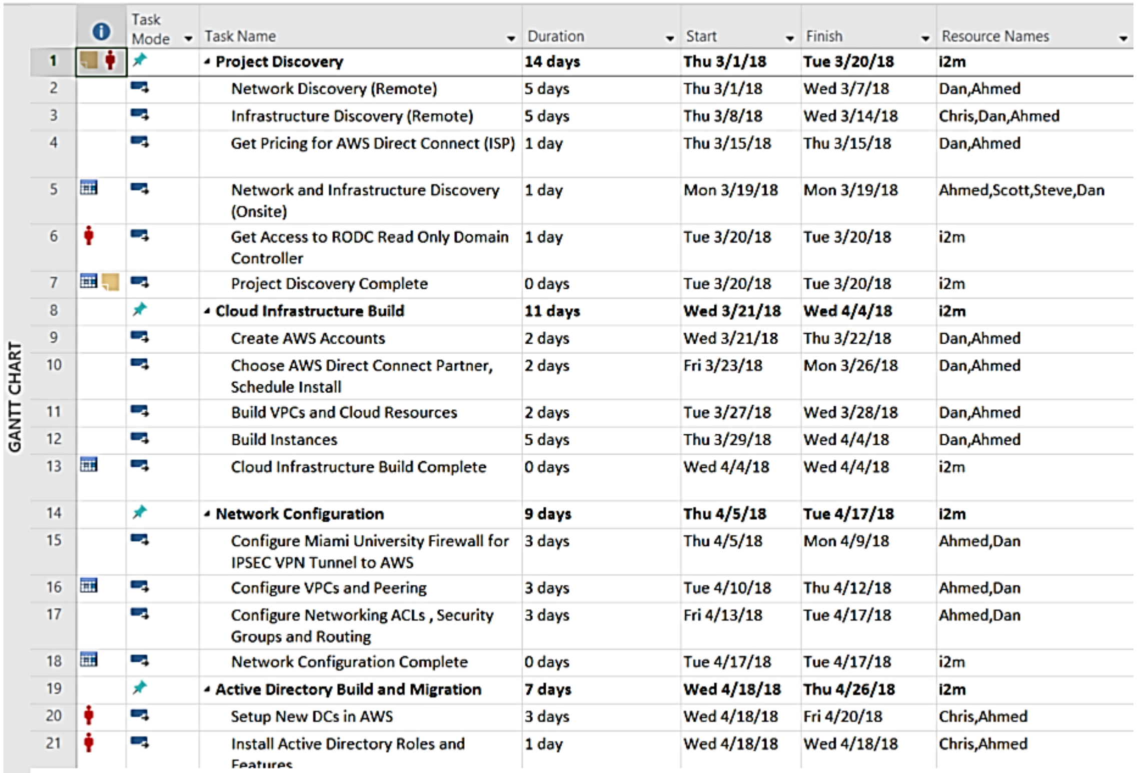
The Project manager will first start by creating a scheduled and detailed task list of the tasks required to complete a project or work. This detailed plan list will have due dates and schedules for specific tasks or project task lists. i2m will give the appropriate access to projects into our Project Management System. The Purchasing Entity can have full visibility to progress, updates and tasks it may be assigned for the project. Purchasing Entities are encouraged to access and see the project plans and timelines as they are created and finalized and approve them before the start of any project.

Timelines for developing, testing, and implementing Solutions for customers

The timeline for each project and solution implementation will be specified by the Project Manager. All relative information will be relayed by the Project Manager to the Contract/Account Manager to make sure all needs are met. The timeline for each solution implementation will vary depending on the size of the organization, the scale of the project, and the availability of the required Purchasing Entities' staff who will need to be involved, and other unknown factors. As for mentioned cloud services accounts can be created between 24-72 hours or longer depending on quantity. To get a solution running in development, testing and then production phases depends on many factors and cannot always be guaranteed. When all the information surrounding a project is given to i2m, i2m will give an estimated time line to the Purchasing Entity on when it can start and when it will be ready for the various stages of the implementation.

Example Project Timeline




GANTT CHART

	ⓘ	Task Mode	Task Name	Duration	Start	Finish	Resource Names
1			**Project Discovery**	**14 days**	**Thu 3/1/18**	**Tue 3/20/18**	**i2m**
2			Network Discovery (Remote)	5 days	Thu 3/1/18	Wed 3/7/18	Dan,Ahmed
3			Infrastructure Discovery (Remote)	5 days	Thu 3/8/18	Wed 3/14/18	Chris,Dan,Ahmed
4			Get Pricing for AWS Direct Connect (ISP)	1 day	Thu 3/15/18	Thu 3/15/18	Dan,Ahmed
5			Network and Infrastructure Discovery (Onsite)	1 day	Mon 3/19/18	Mon 3/19/18	Ahmed,Scott,Steve,Dan
6			Get Access to RODC Read Only Domain Controller	1 day	Tue 3/20/18	Tue 3/20/18	i2m
7			Project Discovery Complete	0 days	Tue 3/20/18	Tue 3/20/18	i2m
8			**Cloud Infrastructure Build**	**11 days**	**Wed 3/21/18**	**Wed 4/4/18**	**i2m**
9			Create AWS Accounts	2 days	Wed 3/21/18	Thu 3/22/18	Dan,Ahmed
10			Choose AWS Direct Connect Partner, Schedule Install	2 days	Fri 3/23/18	Mon 3/26/18	Dan,Ahmed
11			Build VPCs and Cloud Resources	2 days	Tue 3/27/18	Wed 3/28/18	Dan,Ahmed
12			Build Instances	5 days	Thu 3/29/18	Wed 4/4/18	Dan,Ahmed
13			Cloud Infrastructure Build Complete	0 days	Wed 4/4/18	Wed 4/4/18	i2m
14			**Network Configuration**	**9 days**	**Thu 4/5/18**	**Tue 4/17/18**	**i2m**
15			Configure Miami University Firewall for IPSEC VPN Tunnel to AWS	3 days	Thu 4/5/18	Mon 4/9/18	Ahmed,Dan
16			Configure VPCs and Peering	3 days	Tue 4/10/18	Thu 4/12/18	Ahmed,Dan
17			Configure Networking ACLs , Security Groups and Routing	3 days	Fri 4/13/18	Tue 4/17/18	Ahmed,Dan
18			Network Configuration Complete	0 days	Tue 4/17/18	Tue 4/17/18	i2m
19			**Active Directory Build and Migration**	**7 days**	**Wed 4/18/18**	**Thu 4/26/18**	**i2m**
20			Setup New DCs in AWS	3 days	Wed 4/18/18	Fri 4/20/18	Chris,Ahmed
21			Install Active Directory Roles and Features	1 day	Wed 4/18/18	Wed 4/18/18	Chris,Ahmed

Once an SLA or an agreement for POC is in place and cloud services accounts created, i2m will either start the development phase immediately once all stakeholders approve or start on a mutually agreed on date and time. The development phase may take as little as 24 hours or up to a couple of weeks to have ready for testing depended on the solution being developed. It is not in i2m's best interest or the Purchasing Entity to prolong the development phase as long as it meets the requirements of the solution intended. i2m uses templates and automation tools to develop our solutions rapidly and with less human error. The testing phase can last as long as the Purchasing Entity deems fit. After the testing phase and approval of the implementation, an extensive and comprehensive detailed project plan will be formulated to put this testing/QA environment into production with a minimal amount of risk and downtime. This plan will be approved coordinated by all stake holders before production work or tasks are started.

8.3.8

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

- How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.
- How Offeror will maintain discounts at the levels set forth in the contract.

- How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.
- How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

Response:

i2m Procedures to Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein

New manufacturer/service provider's pricing list sheets/catalog will be submitted NASPO ValuePoint and the Purchasing Entities in the future to reflect new services or features and reduced pricing of products/services offerings from the manufacturer or CSP. This will not occur under any circumstance, until new manufacture pricing lists and updated services list are submitted to NASPO ValuePoint for approval according to the terms and conditions set forth in this proposal. Sales staff is trained not supply any new pricing or services information that has not received approval from NASPO ValuePoint and any of its contracted Purchasing Entities.

i2m will maintain discounts at the levels set forth in the contract

Our sales and accounting staff is formally trained with documentation and knowledgebase articles that reference of our sales and accounting policies, process and procedure. i2m accounting staff references our contracts, proposals, agreements and pricing lists and discounts specific to contracted NASPO ValuePoint Purchasing Entities. Sales staff is only allowed to reference and sell products or services listed in the "Cost Proposal" within this RFP. Our Staff is prohibited from selling or referencing products or services not mentioned in this RFP. i2m's Sales and Accounting Staff are trained on utilizing the correct discount rates across each specific product line or CSP in the sales and billing process. The Purchasing Entity will be able to see and quantify these discount values easily and thoroughly through the billing reports i2m and the CSP provide.

i2m will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates

i2m periodically (at least once every month) pulls new pricing catalogs direct from the manufacture and CSPs. We also are included in new letters released by the CSPs detailing any cost reduction or updated services. Once i2m is notified of price reduction or service additions, i2m will contact NASPO and follow the directions specified by the Purchasing Entity to approve new services or update exiting ones from price and description parameters that may have changed.

Member accounts' can also be reviewed on weekly, monthly, quarterly or semi-annual basis according to member's discretion. Member accounts will be reviewed with an assigned account manager. All member's accounts get internally reviewed by i2m on monthly basis for billing and usage purposes.

The nature of the review will be up to the member and may include but not limited to Billing, Cost Management, Governance, Security of Member account(s) and new products/services available from Manufacturers.

Account review rates are specified in Cost Proposal documents.

i2m will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change
i2m will provide transition support to any Purchasing Entity whose operations may be negatively impacted by a service change. There is many cases where a service or solution model may be retired (EOL) or updated significantly where it will impact the cloud service solution, its deployment and configuration. i2m will notify the Purchasing Entity of such changes that may affect them negatively or positively.

In some cases the i2m does not have visibility into the usage of a particular service or does not have visibility to how it is used. The Purchasing Entity should always keep itself updated with the latest in news, technology and any service solution updates or features within their chosen solutions specifically ones that are not managed or maintained by i2m. i2m will can work with the entity to remediate or resolve issues with services that need to be updated or retired. i2m can recommend replacement solutions or services or perform a project plan to migrate to the new services or solution. This assistance will be charged according to rates specified in the "Cost Proposal".

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

Response:
Quality assurance measures
i2m provides an excellent customer service experience by using the best of breed solutions for MSPs for Client Management, Incident Response, Automation, Help Desk and more. i2m

utilizes ConnectWise Suite which empowers Technology Solution Providers to deliver exceptional service more efficiently.

With i2m and ConnectWise we connect everything related to our solutions and customers with in one application. It is the business management platform designed to run our technology solution business and deliver excellent service to our clients.

To achieve superior service delivery we put people first and leave the processes to ConnectWise Manage. With clear lines of communication, error-proof ticketing, powerful documentation. ConnectWise Manage helps i2m deliver it all, so we have the power to efficiently use our resources. We can capture and track every step, maximize visibility, and establish workflows so we can deliver exceptional customer service.

We get to know our business better and how it is operating. We see every vital detail with ConnectWise Manage Reporting. Making strategic, data-driven decisions for our customer service and delivery of our solutions with powerful reporting and informative dashboards. We have a centralized view of every aspect of our business and the clients we manage and deliver services too.

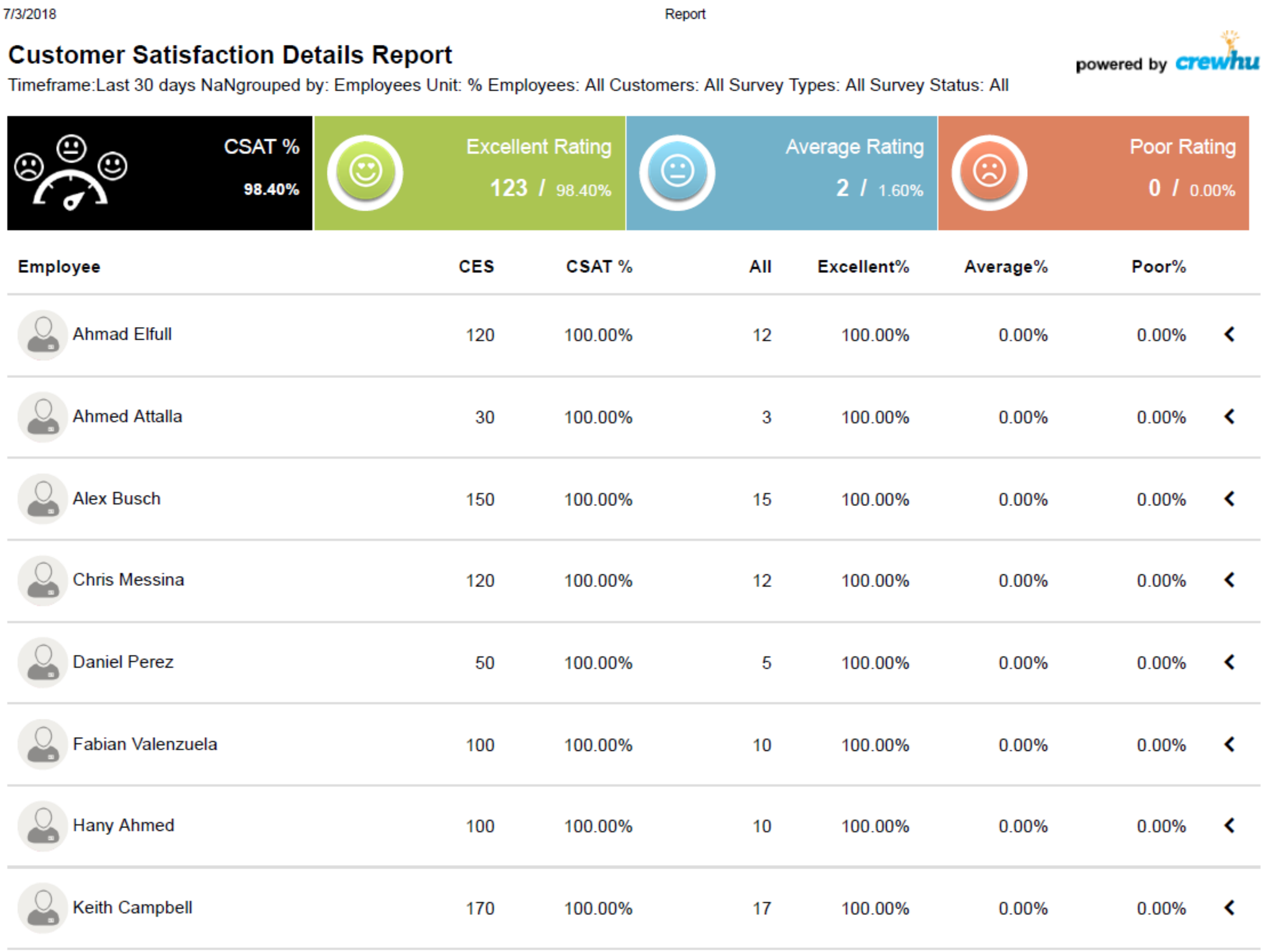
With ConnectWise we have full visibility to billing where we can funnel everything through ConnectWise Manage to make billing more accurate. From tracking time to invoicing and billing, We stay on top of our finances and stop wasting time on manual and repeatable tasks. With built-in automation from ConnectWise Manage, we take advantage of full visibility to deliver invoices on time, eliminate human error and offer world-class service.

We have visibility that keeps everyone on the same page. We can seamlessly transition projects and tasks to keep our communication flowing without ever worrying about accountability and visibility. Allowing every department to work as a single, cohesive team, all from one application.

Also as a supplement to ConnectWise, we use CrewHu a ticket resolution evaluation process that will send the ticket opener a review form after the ticket has been resolved to review the quality of service received. These reviews are optional to the requester and are periodically reviewed by Technical and Executive Managers to address any concerns or poor reviews with the individuals or teams that are responsible, providing constructive and positive feedback so they can remediate the issues concerning the client and prevent any of the same issues from occurring again.

CSAT (Customer Satisfaction) is monitored using CrewHu (ww.crewhu.com) for customer satisfaction and employee engagement. All closed tickets are offered a one click survey with response of Excellent, Average and Poor. Additional metrics are offered and captured with customer engagement in categories of Accuracy, Helpfulness, Knowledge, Proactiveness, Resolution Time and Response Time. All Average and Poor survey results are reviewed by management and corrective actions taken.

Attached is a 30 day CSAT report for a small number of employees:



7/3/2018 Report

Customer Satisfaction Details Report

Timeframe:Last 30 days NaNgrouped by: Employees Unit: % Employees: All Customers: All Survey Types: All Survey Status: All

powered by crewhu

CSAT %	Excellent Rating	Average Rating	Poor Rating
98.40%	123 / 98.40%	2 / 1.60%	0 / 0.00%

Employee	CES	CSAT %	All	Excellent%	Average%	Poor%	
Ahmad Elfull	120	100.00%	12	100.00%	0.00%	0.00%	<
Ahmed Attalla	30	100.00%	3	100.00%	0.00%	0.00%	<
Alex Busch	150	100.00%	15	100.00%	0.00%	0.00%	<
Chris Messina	120	100.00%	12	100.00%	0.00%	0.00%	<
Daniel Perez	50	100.00%	5	100.00%	0.00%	0.00%	<
Fabian Valenzuela	100	100.00%	10	100.00%	0.00%	0.00%	<
Hany Ahmed	100	100.00%	10	100.00%	0.00%	0.00%	<
Keith Campbell	170	100.00%	17	100.00%	0.00%	0.00%	<

Escalation plan for addressing problems and/or complaints

At any time NASPO ValuePoint and its Purchasing Entities need to speak to an executive or escalate an issue for any reason please contact them below. They are available 24/7/365 in the order provided or cc them in an email all at once and someone will respond to your concern asap. Please make sure to reference the proper ticket number in your request for escalation or forward the ticket number as part of your initial request.

Ahmed Attalla	President, i2m.cloud	ahmeda@i2m.cloud	267-240-9097
Scott Miller	COO, i2m	scottm@i2m.solutions	484-238-4118

Steven Grzywinski	President and CTO, i2m	steveg@i2m.solutions	484-433-7136
Hany Ahmed	Tech Services Manager	hanaya@i2m.solutions	267-694-8053

Service Level Agreement (SLA)
Within our client management system ConnectWise we are able to set specific SLAs for each Purchasing Entity defining unique SLAs required by each Entity. SLAs are visible to the Contract Manager and the Client's Business and Technical team. So the team knows which SLAs it is required to meet and stay compliant with. All tickets are subject to SLA as determined by customer and contract. i2m's default SLA is outlined as follows; 1 Hour to respond to ticket, 4 Hours to have a plan and 24 Hours for resolution. Ticket owner has automation applied to alert of missing any SLA targets. Additionally management per service board is alerted to any SLA that hits 75% critical per missing targets. When working on issues or implementing a project the i2m team knows the scope and mandatory minimums defined within each SLA. Our client management platform also uses automated features that inform the ticket holder and/or Business/Contract Manager when any incident or help ticket falls out of the scope SLA requirements and thresholds that are set for that Purchasing Entity. At that time the Contact Manager will get involved and help remedy the situation to ensure the SLA is back to its defined scope.

AWS (IaaS, PaaS, and SaaS offerings) SLA

AWS Support:

Case Severity and Response Times
AWSs goal is to provide an appropriate level of urgency to each case based on the impact to your business or application. Opening cases with the appropriate level of severity will help us get you in touch with the right Support professionals within the target response times.

Severity
General guidance:
You have a general development question, or you want to request a feature.

System impaired:
Non-critical functions of your application are behaving abnormally, or you have a time-sensitive development question.

Production system impaired:
Important functions of your application are impaired or degraded.

Production system down:

Your business is significantly impacted. Important functions of your application are unavailable.

Business-critical system down:
Your business is at risk. Critical functions of your application are unavailable.

AWS Business Premium Support SLA:

- Case Severity and Response Times*
    - General guidance: < 24 hours
    - System impaired: < 12 hours
    - Production system impaired: < 4 hours
    - Production system down: < 1 hour

AWS Enterprise Premium Support SLA:

- Case Severity and Response Times*
    - General guidance: < 24 hours
    - System impaired: < 12 hours
    - Production system impaired: < 4 hours
    - Production system down: < 1 hour
    - Business-critical system down: < 15 minutes

Response Times

AWS target response time will vary based on the impact you tell us the issue is having on your business. We will make every reasonable effort to respond to your initial request within the timeframes in the table below.

AWS SLAs

These are just some of the Services SLAs a full SLA report can be found here: https://aws.amazon.com/legal/service-level-agreements/

- EC2 SLA of at least 99.95% https://aws.amazon.com/compute/sla/
- S3 SLA of at least 99.9% https://aws.amazon.com/s3/sla/
- RDS (PaaS) SLA of at least 99.95% https://aws.amazon.com/rds/sla/
- Amazon DynamoDB of at least 99.99% https://aws.amazon.com/dynamodb/sla/

SaaS Offerings SLA

- DUO: SLA of at least 99.95%

Uptime	Days Credited
< 99.95% - ≤ 99.9% (Duo Care premium only)	3
< 99.9% - ≤ 99.0%	3
< 99.0% - ≤ 95.0%	7

  - < 95.0% 15

- Trend Micro: SLA of at least 99.95%
  - The Service is hosted twenty-four (24) hours a day, seven (7) days a week in Trend Micro's managed public IaaS environment. The Service systems, network, and capacity are continually monitored to provide optimal availability and efficiency to Service customers.

- CloudBerry: SLA of at least 99.95%

- CloudHealth: SLA of at least 99.95%

- Druva: SLA of at least 99.95%
  - Deploy globally in any region for optimal online backup and restore performance 99.5% availability achieved by thorough data replication across multiple availability zones within each region (24 hours per day, 7 days per week) 99.99999% data durability. Designed to sustain the concurrent loss of data in two facilities

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.

Response:
i2m complies it will assign a single Account Manager(lead representative) for each entity that executes a Participating Addendum.

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

Response:
i2m complies and confirms that Customer Service Representative(s) will be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

AWS Premium Support (IaaS, PaaS and SaaS) offerings
These are just some of the Services SLAs a full SLA report can be found here:
https://aws.amazon.com/legal/service-level-agreements/

- Technical Support
  - 24x7 access to Cloud Support Engineers via email, support ticket, chat, and phone

SaaS Offerings Business Support

- DUO: 24/7 access to Support Engineers via email or phone
- Trend Micro: 24/7 access to Support Engineers via email, chat, and phone
- CloudBerry: 24/7 access to Support Engineers via email or support ticket
- CloudHealth: 24/7 access to Support Engineers via email, support ticket, chat, or phone
- Druva: 24/7 access to Support Engineers via email, support ticket, chat, or phone

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

Response:

i2m complies and confirms that Customer Service Representative(s) will be available by phone or email at a minimum, and respond to inquiries within one business day or less. All i2m service offerings also meet the same standards as for mentioned in the response to section 8.4.2 response b.

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

Response:

i2m complies and confirms it provides design and implementation services for the applicable categories and the services offered throughout this RFP.

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

Response:

i2m complies and confirms it provides Installation Services for the applicable categories and the services offered throughout this RFP.

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.

Response:

AWS Shared Responsibility Model:
Within AWS, Customers always maintain full ownership and control of their data during the entire technology lifecycle. This is based on the cloud shared responsibility model. Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment.

AWS responsibility "Security of the Cloud"
AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility "Security in the Cloud"
Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and Amazon S3 are categorized as Infrastructure as a Service (IaaS) and, as such, require the customer to perform all of the necessary security configuration and management tasks. If a customer deploys an Amazon EC2 instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For more detailed information, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Data Protection:
AWS offers you the ability to add an additional layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. This includes:

- Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift
- Flexible key management options, including AWS Key Management Service, allowing you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your keys
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to satisfy compliance requirements

In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.

For more detailed information, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

AWS Regions and Availability Zones

The AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). AWS Regions provide multiple, physically separated and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. These Availability Zones offer AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures. For customers who specifically need to replicate their data or applications over greater geographic distances, there are AWS Local Regions. An AWS Local Region is a single datacenter designed to complement an existing AWS Region. Like all AWS Regions, AWS Local Regions are completely isolated from other AWS Regions. The AWS Cloud spans 55 Availability Zones within 18 geographic Regions and one Local Region around the world.

In addition to replicating applications and data across multiple data centers in the same Region using Availability Zones, you can also choose to increase redundancy and fault tolerance further by replicating data between geographic Regions. You can do so using both private, high speed networking and public internet connections to provide an additional layer of business continuity, or to provide low latency access across the globe.

Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer 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.

Network Monitoring and Protection

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. 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, and unauthorized intrusion attempts. The 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 which 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, worldclass 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 multihomed across a number of providers to achieve Internet access diversity.

- **Man in the Middle (MITM) Attacks**. All of the AWS APIs are available via SSL-protected endpoints which 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 customers 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. Customers 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 arequest via the website at: https://aws-portal.amazon.com/gp/aws/html-formscontroller/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 customer 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 customer inadvertently or maliciously attempting to view another's data, as a standard practice you should encrypt sensitive traffic.

In addition to monitoring, regular vulnerability scans are performed on the host operating system, web application, and databases in the AWS environment using a variety of tools. Also, AWS Security teams subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at: http://aws.amazon.com/security/vulnerability-reporting/

Archiving Data

Amazon Web Services offers a complete set of cloud storage services for archiving. You can choose Amazon Glacier for affordable, non-time sensitive cloud storage, or Amazon Simple Storage Service (S3) for faster storage, depending on your needs. With AWS Storage Gateway and our solution provider ecosystem, you can build a comprehensive, storage solution. Amazon Web Services offers a complete set of cloud storage services for archiving. You can choose Amazon Glacier for affordable, non-time sensitive cloud storage, or Amazon Simple Storage Service (S3) for faster storage, depending on your needs. With AWS Storage Gateway and our solution provider ecosystem, you can build a comprehensive, storage solution. Amazon Glacier and S3 support secure transfer of your data over Secure Sockets Layer (SSL) and can automatically encrypt data at rest using Advanced Encryption Standard (AES) 256-bit symmetric keys. Following a shared security model, AWS's cloud storage solutions provide data protection throughout the infrastructure, allowing you to focus on your applications. AWS cloud storage solutions are designed to simplify the complexity around moving your data. AWS Import/Export enables data transfer from your on-premises infrastructure to Amazon Glacier in a manageable way. AWS Storage Gateway allows you to build a virtual tape library for Amazon S3 or virtual tape shelf for Amazon Glacier, providing cost savings by moving data from S3 to Glacier.

AWS Service and Storage Decommissioning

Before AWS updates or puts a service into end of life. AWS gives the customer ample to time migrate move or upgrade into a new or updated service. AWS will notify the customer when a service or platform reaches its end of life or has a service disruption or a major update. When a storage device and any data has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer 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

i2m data protection procedures

i2m holds data for projects and contracts temporarily throughput the life of the contract or project as determined by the Purchasing Entity and gets stored in a highly secured knowledgebase restricted by network access controls, firewalls and logs for any user activity against that data. There is no information stored of the internal solution databases and client data but rather the framework, technical specifications and architecture diagrams of a contract or project services on which the solution was built.

Disposal of data is key in protecting the clients data before and after implementation of a contract or project by either encrypting, archiving or destroying the contract and project data post implementation or when requested by the Purchasing Entity and any we will follow procedures and policies required by the Purchasing Entity on how it is to be destroyed, archived. i2m has options built into its cloud services offerings that allow data to be encrypted at rest and during transfer and during decommissioning process.

It is encouraged that the entity mention in detail their requested data disposal procedures to i2m prior, during and post implementation to meet the applicable standards.

SaaS Offerings (DUO, Trend Micro, CloudBerry, CloudHealth, Druva)
These SaaS Offerings inherent all of the same security measures as AWS in the majority of SaaS solutions' backend using AWSs (IaaS, PaaS and SaaS) services used to host the Purchasing Entities Data. All of the same Infrastructure bound services inherent the same availability, redundancy, security, features and characteristics of AWS. Similar methods are used to hold, protect, and dispose of data following completion of any contract services.

8.5.2

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

Response:
i2m confirms it will comply to all applicable laws concerning and related to data privacy and security according to the Purchase entities definition of these laws, and commits to abide by these laws and regulations.

Protecting your private information is our priority
We want our website and all other interactions with Include Information Management, Inc. to be useful and informative. We provide our websites as a means for you to obtain information about Include Information Management, Inc. and the ways in which we can help you.

This Privacy Policy applies to the Include Information Management, Inc. web sites (include-im.com, i2mcloud.com, i2m.solutions, i2m.cloud), its ticketing and support system (https://na.myconnectwise.net, https://monitor.i2m.solutions), all general and e-mail correspondence and governs data collection and usage. For the purposes of this Privacy Policy, unless otherwise noted, all references to Include Information Management, Inc.

include all the above areas.

The Include Information Management, Inc. websites are primarily informational sites

Collection of Information

If you are merely visiting one our websites, you are not required to provide any personal information and Include Information Management, Inc. does not collect any personal information about you. If you would like to learn more about Include Information Management, Inc., including without limitation, our services and events, you will have the opportunity to provide basic information via our websites, e-mail, or by phone so we can contact you. You may also be asked for contact information such as your name, company affiliation, job title, physical mailing address, e-mail address and telephone number. With respect to the collection of this information, Include Information Management, Inc. disclaims any legal duty to verify the accuracy of any personal information that you provide to us through our websites or other contact methods with Include Information Management, Inc.

We may also collect and process the following data about you

We may ask you to complete surveys that we use for research purposes, although you do not have to respond to them. Details of your visits to our website, including but not limited to, IP address, traffic data, location data, weblogs and other communication data and the resources that you access. This is statistical data about your browsing actions and patterns, and does not identify any individual. If you contact us, regardless of the method, we may keep a record of that correspondence.

Include Information Management, Inc.'s intent is not to collect any sensitive personal information from you. Sensitive personal information includes but is not limited to: race or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical or mental health, sexual life or criminal record. We request that you do not provide us with sensitive personal information of this nature.

Please keep in mind that if you directly disclose personally identifiable Information or personally sensitive data through our any of our websites public areas, this information may be collected and used by others.

Include Information Management, Inc. encourages you to review the privacy statements of websites you choose to link to from Include Information Management, Inc. so that you can understand how those websites collect, use and share your information. Include Information Management, Inc. is not responsible for the privacy statements or other content on websites outside of the Include Information Management, Inc. website.

Use of your Personal Information

Include Information Management, Inc. collects and uses your personal information to operate its website and deliver the products and services you have requested.

Include Information Management, Inc. may also use your personally identifiable information to inform you of other products or services available from Include Information Management, Inc. and its affiliates. Include Information Management, Inc. may also contact you via surveys to conduct research about your opinion of current services or of potential new services that may be offered.

Include Information Management, Inc. does not sell, rent or lease its customer lists to third parties.

Include Information Management, Inc. may share data with trusted partners to help perform statistical analysis, provide customer support, or arrange for deliveries. All such third parties are prohibited from using your personal information except to provide these services to Include Information Management, Inc., and they are required to maintain the confidentiality of your information.

Include Information Management, Inc. will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Include Information Management, Inc.; (b) protect and defend the rights or property of Include Information Management, Inc.; and, (c) act under exigent circumstances to protect the personal safety of users of Include Information Management, Inc., or the public.

Security of your Personal Information

Include Information Management, Inc. secures your personal information from unauthorized access, use or disclosure.

Children Under Thirteen

Include Information Management, Inc. does not knowingly collect personally identifiable information from children under the age of thirteen. If you are under the age of thirteen, you must ask your parent or guardian for permission to use this website or contact Include Information Management.

Opt-Out & Unsubscribe

We respect your privacy and give you an opportunity to opt-out of receiving announcements of certain information.

Changes to this Statement

Include Information Management, Inc. will occasionally update this Privacy Policy to reflect company and customer feedback. Include Information Management, Inc. encourages you to periodically review this Policy to be informed of how Include Information Management, Inc. is protecting your information.

Contact Information
Include Information Management, Inc. welcomes your questions or comments regarding this Privacy Policy. If you believe that Include Information Management, Inc. has not adhered to this Statement, please contact Include Information Management, Inc. at:

Include Information Management, Inc. - i2m
600 West Germantown Pike, Suite 400
Plymouth Meeting, PA 19462
1-888-991-3814

Please Note:
i2m follows the National Institute for Standards and Technology (NIST) 800-53 security controls for the Federal Information Processing Standard (FIPS) 199 defined by our clients to protect their Personally Identifiable Information (PII), electronic Protected Health Information (ePHI under HIPAA) and Federal Tax Information (FTI under IRS 1075) data in addition to other applicable laws as it applies to data privacy and security. i2m confirms it will comply to all applicable laws concerning and related to data privacy and security according to the Purchase Entities definition of these laws, and commits to abide by these laws and regulations which may override some of applicable privacy policies above.

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.

Response:
i2m and AWS will not have access to any customer data and therefore by default cannot access a Purchasing Entity’s user accounts or data unless specifically provided access by the customer. Neither i2m nor AWS will request access except in 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.

8.6 (E) PRIVACY AND SECURITY

8.6.1

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

Response:
i2m attests, confirms and commits that its solutions comply with the NIST definitions for cloud essentials characteristics, service model, and deployments models, 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 we may receive. All current and future AWS services comply with those definitions outlined in the NIST publication. AWS can support all types of data with its offered services. With its compliance with many industry standards. The remaining SaaS services solutions offered are further detailed with their NIST Definitions and their relative supported Data Risk types. It is recommended that the Purchasing Entity during initial meetings qualify each service offering for the NIST Definitions and Data Risk types that meet the organizations compliance and regulatory requirements.

Please see section 8.1.1 for further detail to this response.

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.

Similar to 8.6.5
Response:
i2m currently hold no certifications as the reseller or solution provider of these services but the cloud solutions provided by the CSPs specified in this RFP meet these compliance government or standards organization security certifications. i2m will strive to meet any compliance required to perform.

AWS Compliance Program
Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- Criminal Justice Information Services(CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act(HIPAA)
- Motion Picture Association of America (MPAA)
- FISMA, DIACAP, and FedRAMP
- Argentina Data Privacy
- CISPE
- FERPA
- DOD CSM Levels 1-5
- PCI DSS Level 1
- FIPS 140-2
- MTCS Level 3
- GDPR
- GLBA
- HIPAA
- HITECH
- IRS 1075
- ITAR
- My Number Act [Japan]
- U.K. DPA - 1988
- VPAT / Section 508
- Privacy Act [Australia]
- Privacy Act [New Zealand]
- PDPA - 2010 [Malaysia]
- PDPA - 2012 [Singapore]
- PIPEDA [Canada]
- Spanish DPA Authorization
- CIS
- CJIS
- CSA
- EU-US Privacy Shield
- FFIEC
- FISC
- FISMA
- G-Cloud [UK]
- GxP (FDA CFR 21 Part 11)
- ICREA
- IT Grundschutz [Germany]
- MITA 3.0

- MPAA
- NIST
- PHR
- Uptime Institute Tiers
- UK Cloud Security Principles

Trend Micro:
PCI DSS, HIPAA & HITECH, NIST 800-53, FEDRAMP

CloudHealth:
Cloudhealth is SOC 2 and GDPR compliant

CloudHealth ingests data from the Participating Entities AWS account. That data is stored in Amazon S3. Since the data is stored in AWS, that data meets all the same government or standards organization security certifications that AWS has complied with.

Duo

- SOC 2
- Duo’s two-factor authentication cryptographic algorithms are validated by NIST under FIPS CAVP. Our NIST certifications are available for review for FIPS 186-3 RSA asymmetric cryptography, FIPS 180-4 SHS/SHA hash families and FIPS 198 HMAC algorithm.
- A DEA-accredited auditor, Drummond Group, LLC, have confirmed that Duo Push satisfies Electronic Prescription of Controlled Substance (EPCS) requirements for two-factor authentication. Duo can also help healthcare organizations meet strong access recommendations for Health Insurance Portability and Accountability Act (HIPAA).
- One-time passcodes generated by any recent version of the Duo Mobile app on iOS 6 and later or by the Duo Mobile app for Windows Phone 8.1/10 version 2.0 are FIPS 140-2 Level 1 compliant by default, and Duo's service works with OATH-compliant FIPS 140-2 validated hardware tokens.
- As a provider of secure access solutions, Duo ensures our customers’ data is protected. As such, is committed to GDPR compliance across our organization.

Druva
The U.S. Cloud First policy requires that government agencies take full advantage of cloud computing to improve IT flexibility, boost operational efficiency and minimize costs — while at the same time complying with the strict standards set by NIST. Druva enables agencies to embrace cloud first, with:

- Built on AWS GovCloud to align with regulations and standards to support agency regulated workloads
- Protection for data in-flight and at-rest with FIPS 140-2 validated encryption
- Granular Role Based Access Control that enforces separation of duties
- FedRAMP Authorized - Moderate, HIPAA and SOC2 audited SaaS service

Cloudberry

CloudBerry uploads backup data to the Participating Entities AWS account. That data is stored in Amazon S3. Since the data is stored in AWS, that data meets all the same government or standards organization security certifications that AWS has complied with.

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.

Response:

Start of Confidential
(Start of Paragraph 4)

End of Confidential
(End of Paragraph 4)

Please see section 8.5.1 for further details to this response

8.6.4

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

Response:
Please refer to the response for sections 8.6.3 and 8.5.1

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.

Response:
AWS Compliance Program
Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, accreditations, and other third-party attestations available on demand.

AWS:
Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance.

- C5 [Germany]
- Cyber Essentials Plus [UK]
- DoD SRG
- ENS High [Spain]
- IRAP [Australia]
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- K-ISMS [Korea]
- MTCS [Singapore]
- SEC Rule 17-a-4(f)
- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- Criminal Justice Information Services(CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act(HIPAA)
- Motion Picture Association of America (MPAA)
- FISMA, DIACAP, and FedRAMP

- Argentina Data Privacy
- CISPE
- DOD CSM Levels 1-5
- PCI DSS Level 1
- FIPS 140-2
- MTCS Level 3
- GDPR
- GLBA
- HITECH
- IRS 1075
- ITAR
- My Number Act [Japan]
- U.K. DPA - 1988
- VPAT / Section 508
- Privacy Act [Australia]
- Privacy Act [New Zealand]
- PDPA - 2010 [Malaysia]
- PDPA - 2012 [Singapore]
- PIPEDA [Canada]
- Spanish DPA Authorization
- CIS
- EU-US Privacy Shield
- FFIEC
- FISC
- FISMA
- G-Cloud [UK]
- GxP (FDA CFR 21 Part 11)
- ICREA
- IT Grundschutz [Germany]
- MITA 3.0
- NIST
- PHR
- Uptime Institute Tiers
- UK Cloud Security Principles

Trend Micro:
PCI DSS, HIPAA & HITECH, NIST 800-53, FEDRAMP

CloudHealth:
CloudHealth is SOC 2 and GDPR compliant

CloudHealth ingests data from the Participating Entities AWS account. That data is stored in Amazon S3. Since the data is stored in AWS, that data meets all the same government or standards organization security certifications that AWS has complied with.

Duo

- SOC 2
- Duo's two-factor authentication cryptographic algorithms are validated by NIST under FIPS CAVP. Our NIST certifications are available for review for FIPS 186-3 RSA asymmetric cryptography, FIPS 180-4 SHS/SHA hash families and FIPS 198 HMAC algorithm.
- A DEA-accredited auditor, Drummond Group, LLC, have confirmed that Duo Push satisfies Electronic Prescription of Controlled Substance (EPCS) requirements for two-factor authentication. Duo can also help healthcare organizations meet strong access recommendations for Health Insurance Portability and Accountability Act (HIPAA).
- One-time passcodes generated by any recent version of the Duo Mobile app on iOS 6 and later or by the Duo Mobile app for Windows Phone 8.1/10 version 2.0 are FIPS 140-2 Level 1 compliant by default, and Duo's service works with OATH-compliant FIPS 140-2 validated hardware tokens.
- As a provider of secure access solutions, Duo ensures our customers' data is protected. As such, is committed to GDPR compliance across our organization.

Druva

The U.S. Cloud First policy requires that government agencies take full advantage of cloud computing to improve IT flexibility, boost operational efficiency and minimize costs while at the same time complying with the strict standards set by NIST. Druva enables agencies to embrace cloud first, with:

- Built on AWS GovCloud to align with regulations and standards to support agency regulated workloads
- Protection for data in-flight and at-rest with FIPS 140-2 validated encryption
- Granular Role Based Access Control that enforces separation of duties
- FedRAMP Authorized - Moderate, HIPAA and SOC2 audited SaaS service

CloudBerry

CloudBerry uploads backup data to the Participating Entities AWS account. That data is stored in Amazon S3. Since the data is stored in AWS, that data meets all the same government or standards organization security certifications that AWS has complied with (HIPPA, FedRamp etc.).

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.

Response:
Please refer to section 8.6.3 for details on internal practices and below for practices by the cloud solutions offered in this RFP.

AWS Config: is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting
Continuous Monitoring

With AWS Config, you are able to continuously monitor and record configuration changes of your AWS resources. Config also enables you to inventory your AWS resources, the configurations of your AWS resources, as well as software configurations within EC2 instances at any point in time. Once change from a previous state is detected, an Amazon Simple Notification Service (SNS) notification can be delivered for you to review and take action.

Continuous Assessment
AWS Config allows you to continuously audit and assess the overall compliance of your AWS resource configurations with your organization’s policies and guidelines. Config provides you with the ability to define rules for provisioning and configuring AWS resources. Resource configurations or configuration changes that deviate from your rules automatically trigger Amazon Simple Notification Service (SNS) notifications that help you identify compliance gaps. You can also take advantage of the visual dashboard to check your overall compliance status and quickly spot non-compliant resources.

Change Management
With AWS Config, you are able to track the relationships among resources and review resource dependencies prior to making changes. Once a change occurs, you are able to quickly review the history of the resource's configuration and determine what the resource’s configuration looked like at any point in the past. Config provides you with information to assess how a change to a resource configuration would affect your other resources, which minimizes the impact of change-related incidents.

Operational Troubleshooting

With AWS Config, you can capture a comprehensive history of your AWS resource configuration changes to simplify troubleshooting of your operational issues. Config helps you identify the root cause of operational issues through its integration with AWS CloudTrail, a service that records events related to API calls for your account. Config leverages CloudTrail records to correlate configuration changes to particular events in your account. You can obtain the details of the event API call that invoked the change (e.g., who made the request, at what time, and from which IP address) from the CloudTrail logs.

Enterprise-wide Compliance Monitoring

With multi-account, multi-region data aggregation in AWS Config, you can view compliance status across your enterprise and identify non-compliant accounts. You can dive deeper to view status for a specific region or a specific account across regions. You can view this data from the Config console in a central account, removing the need to retrieve this information individually from each account, and each region.

Discovery

AWS Config will discover resources that exist in your account, record their current configuration, and capture any changes to these configurations. Config will also retain configuration details for resources that have been deleted. A comprehensive snapshot of all resources and their configuration attributes provides a complete inventory of resources in your account.

Change Management

When your resources are created, updated, or deleted, AWS Config streams these configuration changes to Amazon Simple Notification Service (SNS), so that you are notified of all the configuration changes. AWS Config represents relationships between resources so that you can assess how a change to one resource may impact other resources.

Continuous Audit and Compliance

AWS Config is designed to help you assess compliance with your internal policies and regulatory standards by providing you visibility into the configuration of your AWS resources, and evaluating resource configuration changes against your desired configurations.

Compliance as Code

AWS Config allows you to codify your compliance with custom rules in AWS Lambda that define your internal best practices and guidelines for resource configurations. Using Config, you can automate assessment of your resource configurations and resource changes to ensure continuous compliance and self-governance across your AWS infrastructure.

Troubleshooting

Using AWS Config, you can quickly troubleshoot operational issues by identifying the recent configuration changes to your resources.

Security Analysis
Data from AWS Config enables you to continuously monitor the configurations of your resources and evaluate these configurations for potential security weaknesses. Changes to your resource configurations can trigger Amazon Simple Notification Service (SNS) notifications, which can be sent to your security team to review and take action. After a potential security event, Config enables you to review the configuration history of your resources and examine your security posture.

CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications run on AWS. Customers 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 customer applications and services, and any log files that applications generate. Customers 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. Customers can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. Customers can send their existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time. This helps customers better understand and operate their systems and applications, and they can store their logs using highly durable, low-cost storage for later access.

CloudHealth:

CloudHealth Technologies also helps organizations manage cloud environments through a policy-driven approach and focus on cloud governance. CloudHealth provides support for AWS Config, a powerful building block to allow auditing, compliance management, and support an existing incident management process. For example, customers who identify an open port in a security group can easily isolate when the change was made, who made it, and what additional changes were made.

Together with AWS Config, CloudHealth stores AWS infrastructure configuration history so users can search changes by groups, find historical changes to resources, look at the history of an asset’s configuration, and find out what changed. If the CloudTrail integration is turned on in CloudHealth, configuration changes are also correlated to its original owner. Links to bring you directly to the underlying CloudTrail log items supporting the change are provided in the platform.

Enabling CloudHealth AWS Config support is as easy as turning on the service in the AWS Console to push the log files to an S3 bucket, and directing CloudHealth to collect from that bucket.

CloudHealth and the other CSP offerings in this RFP provides similar features for using your own identity provider listed.

Druva:

- Change Management Features
- Configuration Tracking
- Audit Trail

  With inSync audit trail, you can track the operations of inSync users and administrators. inSync retains audit trail records based on the audit trail retention policy. By default, the audit retention period for a user and an administrator is 30 days.

  Activity types

  - All
    - All activities of all users.
  - Folder shared
    - Activities where users shared users shared folders by using inSync Share.
  - Folder unshared
    - Activities where users stopped sharing previously shared folders.
  - Collaborator added
    - Activities where users were added to the list of collaborators for a shared folder.
  - Collaborator removed
    - Activities where users were removed from the list of collaborators for a shared folder.
  - Collaborator permission changed
    - Activities where permissions for a collaborator on a folder were changed.
  - Link created
    - Activities where users created a download link for a file.
  - Link expired
    - Activities where a download link stopped being active.
  - Link deleted
    - Activities where a user deleted a download link.
  - Data restore
    - Activities where users restored data backed up from the device to a specific location.
  - Data download

    - Activities where users downloaded backup data.
  - Mobile access
    - Activities where users accessed backup data by using their mobile.

DUO:

- Change Management Features
- Configuration Tracking
- Audit Trail

  Easily track user activity and get real-time fraud alerts with our detailed user, administrator and telephony logs. Accessible through our admin panel, you can search and export the logs manually via CSV file, or in real-time to your log management or SIEM systems via our REST API. Learn more about Duo's APIs.

  - Authentication Logs
    - Authentication logs show you where and how users authenticate, with usernames, location, time, type of auth factor and more. Normalize user patterns so you can identify abnormal activity.
  - Administrator Logs
    - Administrator log events let you track the username, time and type of administrator activity, including groups, user, integration and device management. Identify any major admin changes and suspicious activity.
  - Telephony Logs
    - Telephony logs give you insight into the type of telephony event (SMS or phone), phone numbers, and the number of telephony credits used, ensuring you don’t run out of credits.

CloudBerry:

- Change Management Features
- Configuration Tracking
- Audit Trail

  Managed Backup service allows service providers to monitor MBS control panel activity actions for a certain period. With Audit Log you can monitor activity for any changes/updates occurred with:

  - Account
  - User
  - Administrator
  - Backup Destination
  - License
  - Login attempts
  - Monitoring records
  - Package

- Backup/Restore plans

- **TrendMicro:**
  - Change Management Features
  - Configuration Tracking
  - Audit Trail
  - Auditing log feature, help administrators to track events on web console which includes the following:
    - Administrative events
    - Outbreak Defense events
    - Group management events
    - Device management events
    - Configure Policy

8.6.7

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

Response:

i2m uses the least privilege model to grant users and groups only the permissions that are required to perform a task on any cloud hosted data. AWS Identity Access Management (IAM) service is used to perform this task in AWS Environments by either using a customers owned Identity Providers (IDP) or AWS managed IDP (IAM) where users and groups can be managed natively and have strict fine grained access controls, authorization and permissions that can be applied to them and the data and resources they have access to in the AWS eco-system of services.

These Permissions let customers 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 (an explicit deny to all services and resources). By default new created users cannot do anything, not even view their own access keys and permissions. To give a user permission to do something, customers can add the permission to the user or add the user to a group that has the required permission. IAM also enables you to add specific conditions such as time of day to control how a user can use AWS, their originating IP address, whether they are using SSL, or whether they have authenticated with a multi-factor authentication (MFA) device.

Manage access control for mobile applications with Web Identity Providers

You can enable your mobile and browser-based applications to securely access AWS resources by requesting temporary security credentials that grant access only to specific AWS resources for a configurable period of time.

IAM can be used to grant your employees and applications federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0,

CloudHealth and the other CSP offerings in this RFP provides similar features for using the Purchasing Entities own identity provider listed. Where customers can also define constraints and restriction based on the Users/Security Group in their own IDPs like LDAP/AD environments. For example restricting them to certain functions within the SaaS service or only allow access to certain accounts or resources and sensitive data.

CloudHealth:

- SSO with your own identity provider (IDP) (e.g. ADFS) public identity services and (IDPs)(i.e. Google).
- SAML 2.0
- User Access control managed natively with fine grain permissions and polices
- Secure Account Access Protocols
- Audit Trail

DUO:

- SSO with your own identity provider (IDP)
- SAML 2.0
- User Access control managed natively with fine grain permissions and polices
- Encryption of data and rest and in transit.
- Audit trail

CloudBerry:

- SSO with LDAP and AD Integration
- User Access control managed natively with fine grain permissions and polices
- Encryption of data at rest and in transit
- Audit Trail

TrendMicro:

- SSO with LDAP and AD integration
- User Access control managed natively with fine grain permissions and polices
- Audit Trail

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.

Response:
Please reference response for section 8.3.2 details i2m's and other SaaS Solutions incident response protocol and procedures

AWS's Incident response procedure:
Incident Response:
The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution. Company-Wide Executive Review Amazon's Internal Audit group has recently reviewed the AWS services resiliency plans, which are also periodically reviewed by members of the Senior Executive management team and the Audit Committee of the Board of Directors.

Communication:
AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees; regular management meetings for updates on business performance and other matters; and electronics means such as video conferencing, electronic mail messages, and the posting of information via the Amazon intranet.

AWS has also implemented various methods of external communication to support its customer base and the community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers 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 customer support team and proactive alerts to any customer 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.

Response:
AWS (IaaS, SaaS and PaaS offerings)
i2m inherits AWS's Infrastructure Security Controls both physical and virtual
AWS Security Responsibilities Amazon Web Services is responsible for protecting the

global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS's number one priority, and while you can't visit our data centers or offices to see this protection firsthand, we provide several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations (for more information, visit (aws.amazon.com/compliance). Note that in addition to protecting this global infrastructure, AWS is responsible for the security configuration of its products that are considered managed services. Examples of these types of services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces, and several other services. These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed. For these services, AWS will handle basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery. For most of these managed services, all you have to do is configure logical access controls for the resources and protect your account credentials. A few of them may require additional tasks, such as setting up database user accounts, but overall the security configuration work is performed by the service.

Customer Security Responsibilities With the AWS cloud, you can provision virtual servers, storage, databases, and desktops in minutes instead of weeks. You can also use cloud-based analytics and workflow tools to process your data as you need it, and then store it in your own data centers or in the cloud. Which AWS services you use will determine how much configuration work you have to perform as part of your security responsibilities. AWS products that fall into the well-understood category of Infrastructure as a Service (IaaS)—such as Amazon EC2, Amazon VPC, and Amazon S3—are completely under your control and require you to perform all of the necessary security configuration and management tasks. For example, for EC2 instances, you're responsible for management of the guest OS (including updates and security patches), any application software or utilities you install on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. These are basically the same security tasks that you're used to performing no matter where your servers are located.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you the Purchasing Entity defines. 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 use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

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

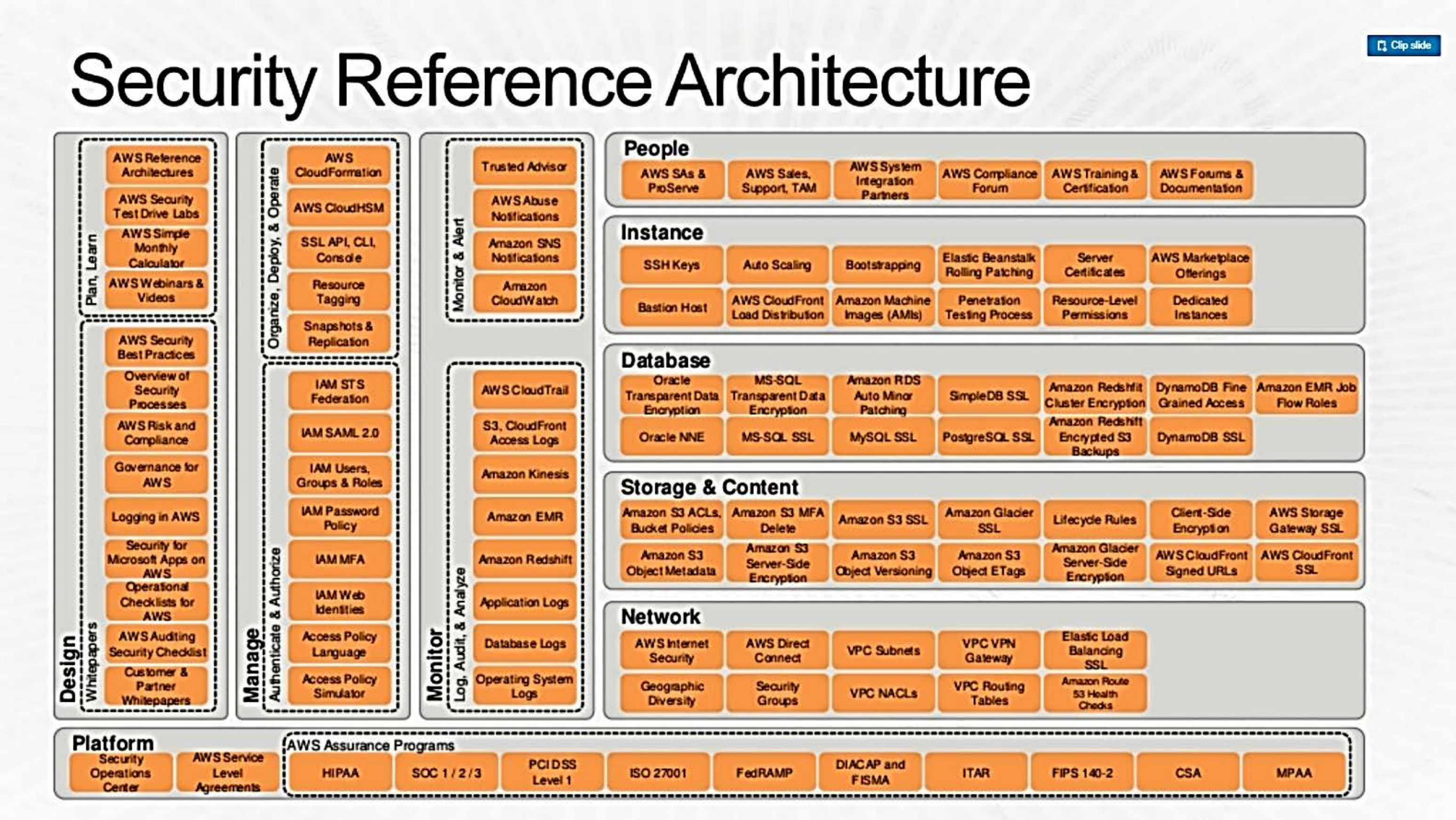
Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS Cloud as an extension of your corporate data center.

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).

Response:

The Reference Security Architecture for AWS IaaS, PaaS and SaaS services offerings:
(please zoom in as necessary for a better view)



Security Reference Architecture

Design
Plan, Learn
AWS Reference Architectures
AWS Security Test Drive Labs
AWS Simple Monthly Calculator
AWS Webinars & Videos
Whitepapers
AWS Security Best Practices
Overview of Security Processes
AWS Risk and Compliance
Governance for AWS
Logging in AWS
Security for Microsoft Apps on AWS
Operational Checklists for AWS
AWS Auditing Security Checklist
Customer & Partner Whitepapers

Manage
Organize, Deploy, & Operate
AWS CloudFormation
AWS CloudHSM
SSL API, CLI, Console
Resource Tagging
Snapshots & Replication
Authenticate & Authorize
IAM STS Federation
IAM SAML 2.0
IAM Users, Groups & Roles
IAM Password Policy
IAM MFA
IAM Web Identities
Access Policy Language
Access Policy Simulator

Monitor
Monitor & Alert
Trusted Advisor
AWS Abuse Notifications
Amazon SNS Notifications
Amazon CloudWatch
Log, Audit, & Analyze
AWS CloudTrail
S3, CloudFront Access Logs
Amazon Kinesis
Amazon EMR
Amazon Redshift
Application Logs
Database Logs
Operating System Logs

People
AWS SAs & ProServe
AWS Sales, Support, TAM
AWS System Integration Partners
AWS Compliance Forum
AWS Training & Certification
AWS Forums & Documentation

Instance
SSH Keys
Auto Scaling
Bootstrapping
Elastic Beanstalk Rolling Patching
Server Certificates
AWS Marketplace Offerings
Bastion Host
AWS CloudFront Load Distribution
Amazon Machine Images (AMIs)
Penetration Testing Process
Resource-Level Permissions
Dedicated Instances

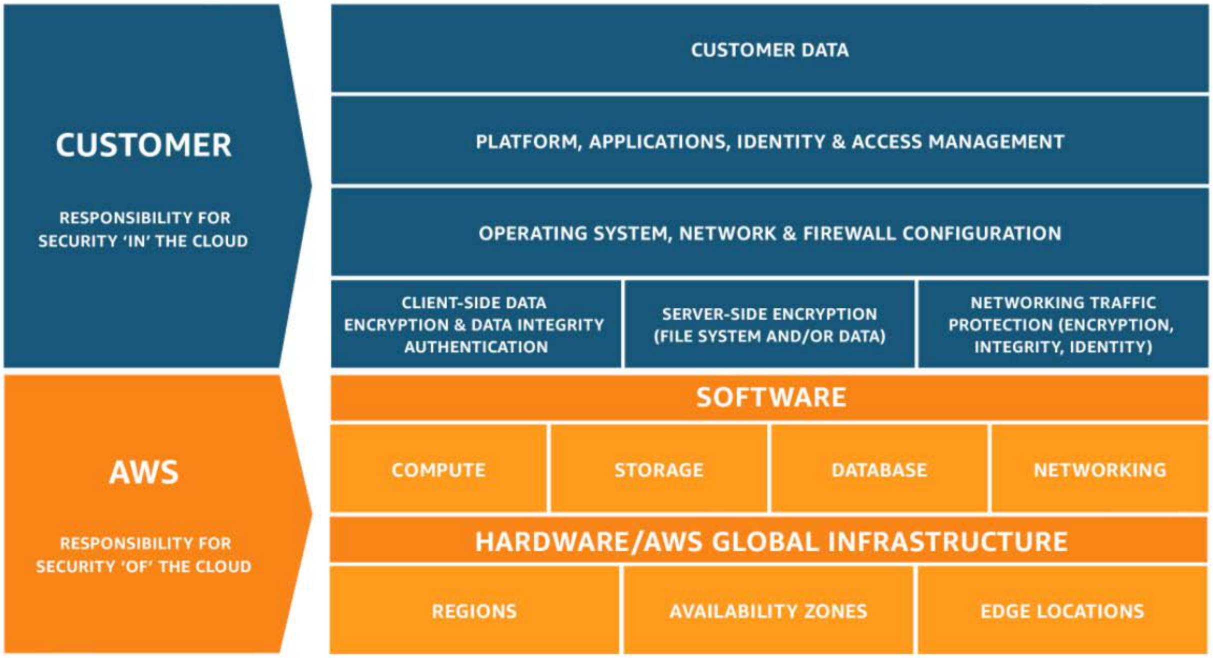
Database
Oracle Transparent Data Encryption
MS-SQL Transparent Data Encryption
Amazon RDS Auto Minor Patching
SimpleDB SSL
Amazon Redshift Cluster Encryption
DynamoDB Fine Grained Access
Amazon EMR Job Flow Roles
Oracle NNE
MS-SQL SSL
MySQL SSL
PostgreSQL SSL
Amazon Redshift Encrypted S3 Backups
DynamoDB SSL

Storage & Content
Amazon S3 ACLs, Bucket Policies
Amazon S3 MFA Delete
Amazon S3 SSL
Amazon Glacier SSL
Lifecycle Rules
Client-Side Encryption
AWS Storage Gateway SSL
Amazon S3 Object Metadata
Amazon S3 Server-Side Encryption
Amazon S3 Object Versioning
Amazon S3 Object ETags
Amazon Glacier Server-Side Encryption
AWS CloudFront Signed URLs
AWS CloudFront SSL

Network
AWS Internet Security
AWS Direct Connect
VPC Subnets
VPC VPN Gateway
Elastic Load Balancing SSL
Geographic Diversity
Security Groups
VPC NACLs
VPC Routing Tables
Amazon Route 53 Health Checks

Platform
Security Operations Center
AWS Service Level Agreements
AWS Assurance Programs
HIPAA
SOC 1 / 2 / 3
PCI DSS Level 1
ISO 27001
FedRAMP
DIACAP and FISMA
ITAR
FIPS 140-2
CSA
MPAA

Shared Responsibility Security model:


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

SECURE DESIGN

SITE SELECTION

Prior to choosing a location, AWS performs initial environmental and geographic assessments. Data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our Availability Zones are built to be independent and physically separated from one another.

REDUNDANCY

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, 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.

AVAILABILITY

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

CAPACITY PLANNING

AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

BUSINESS CONTINUITY & DISASTER RECOVERY

BUSINESS CONTINUITY PLAN

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

PANDEMIC RESPONSE

AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

PHYSICAL ACCESS

EMPLOYEE DATA CENTER ACCESS

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

THIRD-PARTY DATA CENTER ACCESS

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

AWS GOVCLOUD DATA CENTER ACCESS

Physical access to data centers in the GovCloud (US) region is restricted to employees who have been validated as being US citizens.

MONITORING & LOGGING

DATA CENTER ACCESS REVIEW

Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

DATA CENTER ACCESS LOGS

Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

DATA CENTER ACCESS MONITORING

We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

SURVEILLANCE & DETECTION

CCTV

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

DATA CENTER ENTRY POINTS

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

INTRUSION DETECTION

Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

DEVICE MANAGEMENT

ASSET MANAGEMENT

AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

MEDIA DESTRUCTION

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

OPERATIONAL SUPPORT SYSTEMS

POWER

Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

CLIMATE AND TEMPERATURE

AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

FIRE DETECTION AND SUPPRESSION

AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

LEAKAGE DETECTION

In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

INFRASTRUCTURE MAINTENANCE

EQUIPMENT MAINTENANCE

AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

ENVIRONMENT MANAGEMENT

AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

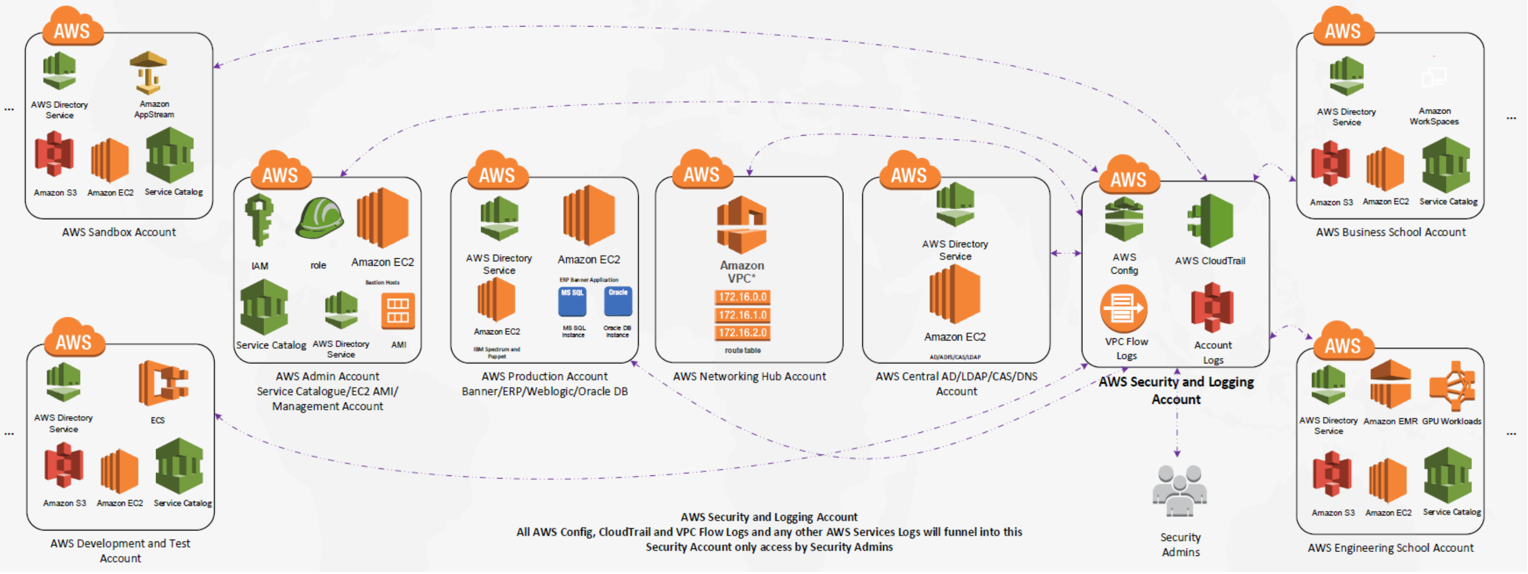
GOVERNANCE & RISK

ONGOING DATA CENTER RISK MANAGEMENT

The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

THIRD-PARTY SECURITY ATTESTATION

Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.



This diagram shows an example of an AWS Security Account which logs all activity and security information from IaaS, SaaS and PaaS Services within the AWS eco-system for a large organization deployments of AWS Solutions.

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.

Response:

i2m Background Checks:

i2m conduct Full Background Checks on all of our employees prior to them being hired and we do not hire anyone with a prior criminal record. Background Checks can be furnished on-demand or conducted at will by NASPO ValuePoint or its Purchasing Entities. i2m will comply with any security procedures or checks required to perform, according to policies and procedures set by the Purchasing Entity and NASPO ValuePoint.

For all DOD and Federal clients only authorized US Citizens only are allowed access to any Federal Government client data and are authorized to do any work for the US Federal Government.

AWS Background Checks:

AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and commensurate with the employee's position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

Druva employs US citizens only for work in the Federal Government Sector

More detailed information on AWS and the remaining SaaS solution offerings background checking procedures can be available on demand.

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.

Response:
i2m can encrypt our customer data at rest and transfer for Purchasing Entity Information on our systems or through the use of its cloud solution offerings in this RFP which include many features for encrypting data at rest and transfer.

Data at Transfer:
Network Security
The AWS network has been architected to permit you to select the level of security and resiliency appropriate for your workload. To enable you to build geographically dispersed, fault-tolerant web architectures with cloud resources, AWS has implemented a world-class network infrastructure that is carefully monitored and managed.

Secure Network Architecture
Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACL Manage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.

Secure Access Points:
AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows you to establish a secure communication session with your storage or compute instances within AWS. To support customers with FIPS cryptographic requirements, the SSL-terminating load balancers in AWS GovCloud (US) are FIPS 140-2-compliant. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing

edge of the AWS network. These connections each have dedicated network devices.

Transmission Protection
You can connect to an AWS access point via HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. For customers who require additional layers of network security, AWS offers the Amazon Virtual Private Cloud (VPC), which provides a private subnet within the AWS cloud, and the ability to use an IPsec Virtual Private Network (VPN) device to provide an encrypted tunnel between the Amazon VPC and your data center. For more information about VPC configuration options, refer to the Amazon Virtual Private Cloud (Amazon VPC) Security section below.

Security of Data at Rest for AWS Services and other SaaS solution offerings in this RFP:

Please see response to section 8.1.1 and 8.9.1 further detail a response to this section to address the Services that have encrypting capabilities and what they entail at rest using Server/Service Side Encryption and Client Side Encryption.

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.

Response:
Please see response for section 8.3.2 which addresses the response to this section relative to all breaches not limited to cardholders data breach.

Amazon Web Services (AWS) is certified as a PCI DSS 3.2 Level 1 Service Provider, the highest level of assessment available. The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA). The PCI DSS Attestation of Compliance (AOC) and Responsibility Summary are available to customers by using AWS Artifact, a self-service portal for on-demand access to AWS compliance reports.

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 de-provisioning 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.

Response:

When a service reaches end of life or needs to be de-provisioned i2m will assist the Purchasing Entity in this event. i2m will provide transition support to any Purchasing Entity whose operations may be negatively impacted by a service change or disruption. There is many cases where a service or solution model may be retired (EOL) or updated significantly where it will impact the cloud service solution, its deployment and configuration. i2m will notify the Purchasing Entity of such changes that may affect them negatively or positively. The Purchasing Entity will also receive direct notifications from the Cloud Solutions Provider (i.e. AWS, Druva, DUO, CloudBerry, CloudHealth, Trend Micro) of any unplanned and planned maintenance, service disruption and service decommissioning events. Purchasing Entity can manages these changes or de-provisioned tasks themselves as well without i2m involvement.

In some cases the i2m does not have visibility into the usage of a particular service or does not have visibility to how it is used. The Purchasing Entity should always keep itself updated with the latest in news, technology and any service solution updates or features within their chosen solutions, specifically ones that are not managed or maintained by i2m. i2m can work with the entity to remediate or resolve issues with services that need to be updated or retired. i2m can recommend replacement solutions or services or perform a project plan to migrate to the new services or solution. This assistance will be charged according to rates specified in the “Cost Proposal”.

AWS Service and Storage Decommissioning:

Before AWS updates or puts a service into end of life. AWS gives the customer ample to time migrate move or upgrade into the a new services. AWS will notify the customer when a service or platform reaches its end of life or has a service disruption or major update. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer 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.

Disposal of data is key in protecting the clients data before and after implementation of a project by either encrypting, archiving or destroying the projects data post implementation when requested by the Purchasing Entity.

The Purchasing Entity has full control over its own data, where project/solution data can be deleted or services de-provisioned at the will.

It is encouraged that the entity mention in detail their requested data disposal procedures to i2m prior, during and post implementation to meet the applicable standards.

i2m maintains security of the data during this phase of an SLA:

AWS services is known for its data portability practices and all AWS and other CSP services allow you to export data to traditional formats for use by the Purchasing Entity as necessary. The Cloud Solutions data can also be exported very easily and natively within each platform to traditional formats that can be later encrypted archived or destroyed by the Purchasing Entity. Data can be easily mirrored and replicated throughout this process or phase by utilizing cloud native or custom solutions. Security can be maintained as well within the solution during this process. i2m can assist the Purchasing Entity in formulating and executing a project plan with policies and procedures that need to be met by the Purchasing Entity to migrate or export data to a new solution or services or disposal of the service/solutions data.

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.

Response:
All the Cloud Services Solutions offered by i2m, have control options to export any customer/client data externally to many industry standard sources that may include on-premise or to several different cloud services providers or solutions.

AWS is known for its data portability practices and all AWS services and other CSP services offered allow you to export data to traditional formats for use by the Purchasing Entity as necessary. AWS for example has an AWS Import/Export service and several other services that allows you to export data (i.e. Server Images, Object Data, Databases, EBS Volumes) with encryption capabilities. The data when transmitted or transported the data will be encrypted by either client solutions or by use of a CSPs native encryption methods which include self-managed encryption keys. AWS services includes AWS Snowball which is a 40 TB – 80 TB military grade storage device, which is and is used import and export massive amounts of data into AWS and Out in an encrypted manner. This bypasses any internet bandwidth inefficiencies in getting large amounts of data returned back to the Purchasing Entity rapidly. The process to export large amounts of data is a very efficient and is a cost effective way to transport data to any global location defined by the Purchasing Entity.

i2m can assist the Purchasing Entity in formulating and executing a project plan with policies and procedures that need to be met by the Purchasing Entity to return data securely and efficiently from any of the Cloud Solutions offered in this RFP. As all the cloud solutions offer this capability natively and via custom solutions.

8.8 (E) SERVICE OR DATA RECOVERY

8.8.1

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

a. Extended downtime.
b. Suffers an unrecoverable loss of data.
c. Offeror experiences a system failure.
d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Response:
Please see section 8.8.2 for the response to this section which describes in full details responses to points a, b, c, d, e of this section.

8.8.2

Describe your methodologies for the following backup and restore services:

a. Method of data backups
b. Method of server image backups
c. Digital location of backup storage (secondary storage, tape, etc.)
d. Alternate data center strategies for primary data centers within the continental United States.

Response:
All of the SaaS Solutions offered follow several of these basic features in a backup and disaster recovery solution specific to AWS, CloudBerry and Druva,

The following Characteristics are observed:

Network Connectivity

- Bandwidth and Latency to/from remote backup resources from The Purchasing Entity sites is adequate (i.e. cloud/local to local/cloud, local/cloud to colocation/branch)
- i2m recommends an AWS Direct Connect a dedicated Ethernet connection to the AWS eco-system, or other providers it decides to use for its object storage..

Recovery Time Objects (RTO)

- FULL Backup restore time objective (RTO)(time it takes to restore a full backup from Local/Cloud Storage) will vary dependent on adequate network bandwidth from minutes to a few hours (i.e. 4 hours) or greater depending on data size and bandwidth/latency in-between the source and destination nodes.

- INCREMENTAL Backup restore time objective (RTO) (time it takes to restore an incremental backup from Local/Cloud Storage) will vary from minutes to greater depending on data size and network bandwidth/latency available in-between the source and destination nodes during the time of a restore.

Recovery Point Objective (RPO)

- FULL Backup frequency (RPO) *Weekly with 6 recover points every week a full backup is taken (time and frequency of backups can be changed or modified to include more daily/weekly/monthly/etc. recover points/versions)*
  These are just baselines

- INCREMENTAL Backup frequency: *Daily with 3 recover points every 8 hours a backup is taken (time and frequency of backups can be changed or modified to include more daily recover points/versions or real-time backups).*
  These are just baselines

Retention:

Example 90 – days' worth of backups can have multiple version with in them with up to the minute real-time versions of objects (i.e. server images/files) (more or less days of retention can be applied to the backup data) and solutions allows for automatic archival an purge options, and deduplication built in,

Functional Area Design Considerations

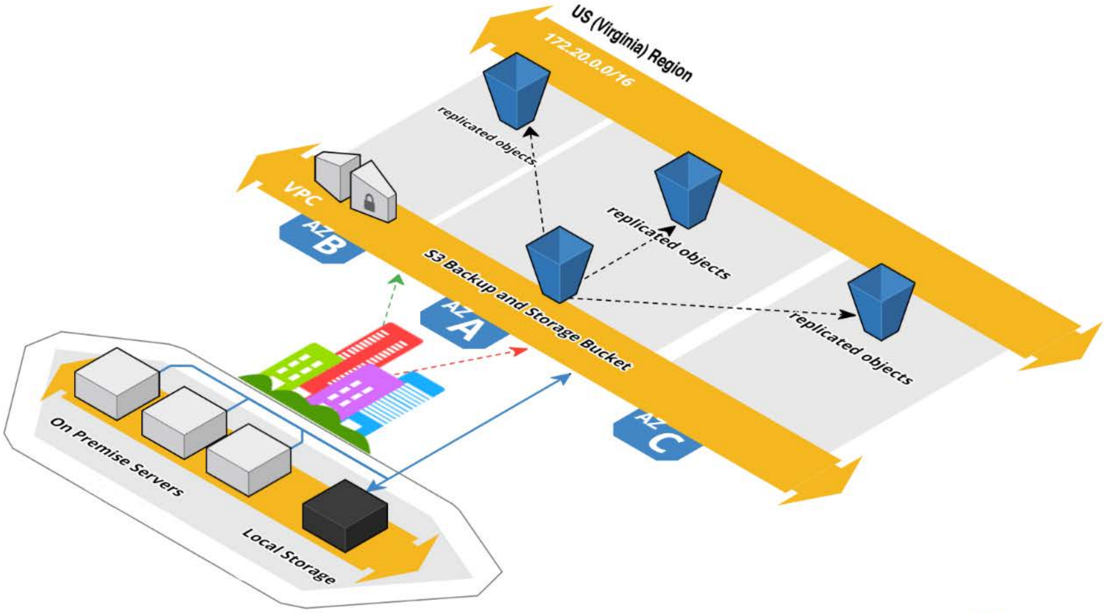
- <u>Internet</u>

  - Internet Speed Recommended 1/1 Gbps

- <u>Local Infrastructure</u>
  - Local Switches/Routers documented and organized if needed
  - Local Network Infrastructure adequate for high bandwidth (1GB preferred internal node to node)
  - Local backup storage device be placed in rack in a network location that closest/highest bandwidth to all the servers being backup up as much as possible.

- <u>Amazon Web Services (S3 cloud remote storage environment)</u>
  - AWS accounts established owned by The Purchasing Entity linked to i2m
  - Public access is not allowed (if required)

    - Accounts only accessible by i2m Certified Cloud Architects (if required) or equivalent The Purchasing Entity personnel.

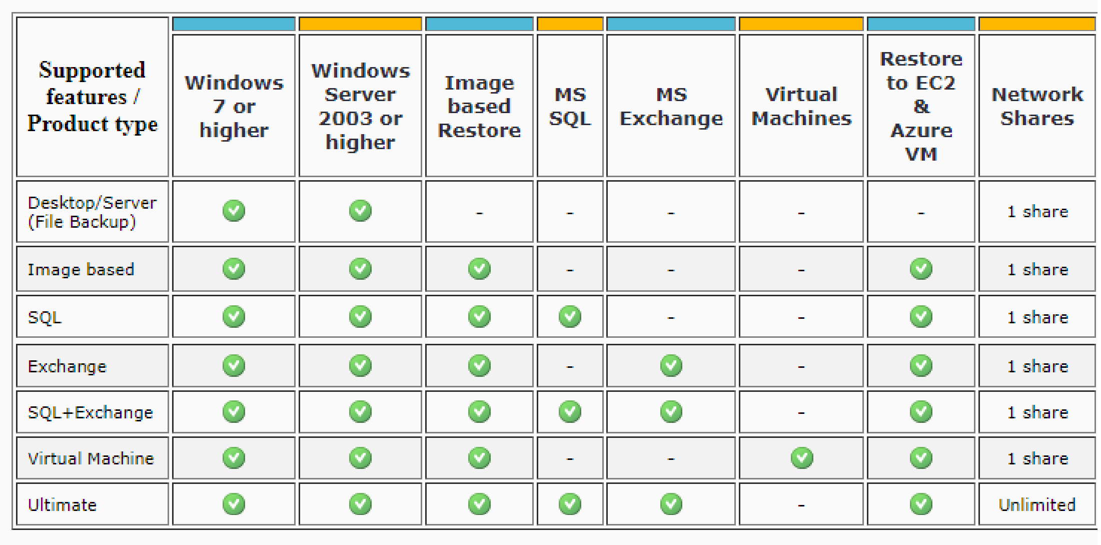


Cloud Backup and Disaster Recovery (i.e. us-east-2 Ohio and us-east-1 Virginia AWS regions):

- AWS S3/Glacier Multi Availability Zone Architecture (Availability Zones (AZs) are datacenters within a region "~50" miles apart from each other) for Durability, Redundancy, Fault Tolerance, High Availability and Disaster Recovery (features below)
- Data is replicated to multiple AZ's; 2 or more (typically a 3 AZ replication for each data object stored)
- Cross Region Replication of data for e.g. to Virginia or California Region is possible providing a higher level of geographic separation from primary data for organizations that need to meet this demand.
- This data can also be distributed global or across the US only for rapid access by any government entity by using the nearest AWS edge location using Amazon CloudFront service (CDN Network).

- Cloud and On-Premise Backup and Disaster Recovery Solution
    - Domain Controllers
        - Daily and Weekly Image and Volume/Disk snapshots
        - Daily Microsoft Active Directory Backups of system state to local storage drive on both primary and secondary DCs

  - Daily Backups of Microsoft Active Directory Backups copied to local and cloud storage for easy restore
  - Daily file backup to multiple alternative availability zones (3 recovery points)
  - Monthly Full Backups
  - 90-day Retention history and restore points
- Data and/or application machines
  - Daily and Weekly Image and Volume/Disk snapshots
  - Daily file backup to multiple alternative availability zone (3 recovery points)
  - Monthly Full Backups
  - 90-day retention history and restore points
- Database machines
  - Daily and Weekly Image and Volume/Disk snapshots
  - Daily file backup to multiple alternative availability zones (3 recovery points)
  - Hourly (or less if required) transaction logs and Daily Full Backups of databases (MySQL/SQL etc.)
  - Monthly Full Backups
  - 90-day retention history and restore points
- CloudBerry Backup Agents
  - Each agent is installed on the machine needing to be backed up
  - Or agent lives on a central machine which is used to backup network shares on SANs, NASs or Windows Server Shares
  - There several Different Agent versions or types depending on the type of the data or solution your backing up
    - Ultimate:
    - Desktop/Server (File Backup): Windows, Mac, Linux
    - MS SQL Server
    - MS Exchange
    - MS SQL Server + MS Exchange
    - Image Based and Restore to AWS EC2 or Azure VM
    - Virtual Machine
    - Virtual Machine Socket
    - Dedup Server



Supported features / Product type	Windows 7 or higher	Windows Server 2003 or higher	Image based Restore	MS SQL	MS Exchange	Virtual Machines	Restore to EC2 & Azure VM	Network Shares
Desktop/Server (File Backup)	✓	✓	-	-	-	-	-	1 share
Image based	✓	✓	✓	-	-	-	✓	1 share
SQL	✓	✓	✓	✓	-	-	✓	1 share
Exchange	✓	✓	✓	-	✓	-	✓	1 share
SQL+Exchange	✓	✓	✓	✓	✓	-	✓	1 share
Virtual Machine	✓	✓	✓	-	-	✓	✓	1 share
Ultimate	✓	✓	✓	✓	✓	-	✓	Unlimited

CloudBerry and Druva Backup common Specifications

- Backup and Disaster Recover for all Local and Cloud Resources with 90-day retrieval history (more or less can be accommodated)
- Cloud Storage Data Replicated to multiple AZ's within the region
- Local Storage Data is replicated to Local Physical Storage (NAS)
- Local Storage Device up to ~48TB of Data more space can be added up to 96TB (3 Year Warranty)
- AWS Glacier/S3 for Archiving and Backup of Old Data/Unused Data and Live Data respectively
- RPO: 3 Daily Recovery Points (24 hours) (schedule to be determined, default every 8 hours), and all RPO within 90-day retrieval history (Daily-Weekly-Monthly-90 days)
- RTO: Will be immediate (within minutes) and up to few hours for all data, dependent on the size/amount of the data needed to be restored and bandwidth of the connection between local and cloud storage
- 256-Bit AES Encrypted Data at rest and SSL encryption during transfer
- Automated Offsite Archival Storage of specified data by (date/size/last accessed/last modified) or manual selection
- Archival Storage can be written to any local portable media and restored from cloud storage is instantly accessible and searchable independently and via the backup solution
- Allow for the backup of open/locked files via Microsoft VSS and 3rd party VSS
- Retention plans can be specified for archival data which can allow for automatic purging of old data or keep as long as needed
- Permanent retention for live and archival data can be set
- Authorized The Purchasing Entity personnel will be granted full backend access to on-site/offsite storage devices and repositories for independent restores of any data without using the Backup Solution

- Backup Solution supported for 3 years (solution can accommodate more)
- See below for all features and specifications
- Quarterly Restore and Data Consistency Check testing/analysis (more can be accommodated)

CloudBerry and Druva Backup Disaster Recovery Specifications

- Disaster Recover for all Local and Cloud Resources with 90-day retrieval history (more can be accommodated)
- Retrieval history includes Daily, Weekly, Monthly Recovery Points for Images and Snapshots
- Ability to restore Images/Snapshots from Daily, Weekly or Monthly backups
- Ability to Restore to and from any physical or virtual machines
- Ability to Restore VM/Physical Machines to on premise infrastructure (physical/virtual machine)
- Ability to Restore VM/Physical Machines to cloud infrastructure (AWS (recommended) / MS Azure) (restore to EC2 or Azure) **
- Cloud Storage Data Replicated to multiple AZ's within the region
- Local Storage Data is replicated to Local Physical Storage (NAS)
- 256-Bit AES Encrypted Data at rest and SSL encryption at transfer
- Disaster Recover Solution supported for 3 years (solution can accommodate more)
- Semi-Annual Image and Snapshot Recover and Consistency DR testing (more can be accommodated)

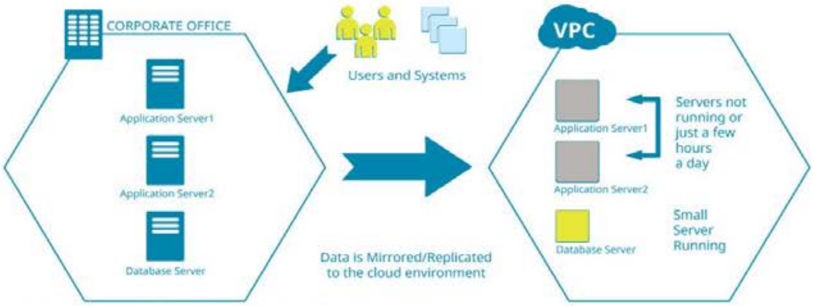
**The Ability to restore snapshots or images or entire site to remote site (AWS VPC) (restore to EC2) will be enabled and tested for verification only on a few critical machines. Restores to on premise are covered as long as The Purchasing Entity provides server capacity in the on-premise infrastructure. In the scenario where on-premise infrastructure has failure/outage and machine(s) need to be recovered off-premise (to the AWS cloud) for e.g. The Purchasing Entity will incur charges for running their infrastructure in the cloud remote site during a DR scenario. These charges will correspond with actual usage on AWS cloud charged by i2m according to AWS Services Cost Proposal in this RFP. The time/materials required for i2m Engineers manage migrating or restoring the local infrastructure to cloud infrastructure with the assistance of The Purchasing Entity Engineers is provided Cost Proposal in this RFP.

Disaster Recovery Plans

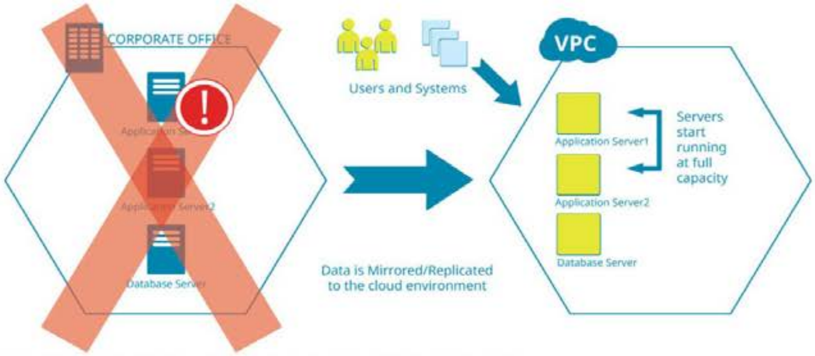
Pilot Light, Warm Standby, Hot Standby, Active/ Active Plans can be requested to implement.

OPTION 2: The Pilot Light Plan

While backup and restore are focused on data, pilot light includes applications. Companies only provision core infrastructure needed for critical applications. When disaster strikes, using Amazon EC2 instances and other automation services, we can quickly provision the remaining environment for production.



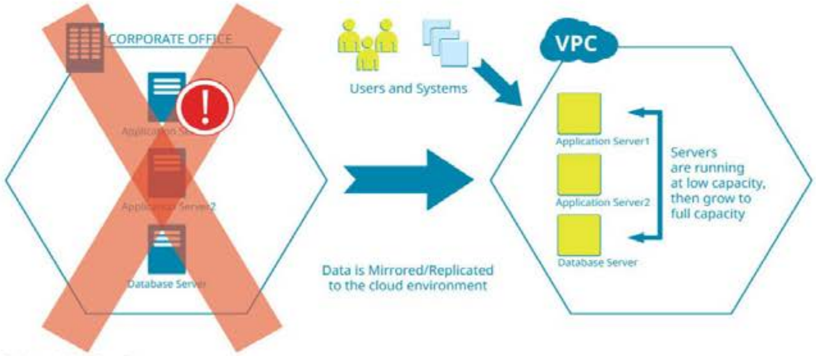
Stage 1: Users and systems access your local corporate office environment.
Data is replicated every 24 hours to the cloud environment



Stage 2: Disaster situation occurs, systems start and all users and systems are pointed to access the cloud disaster recovery environment with minimal downtime.

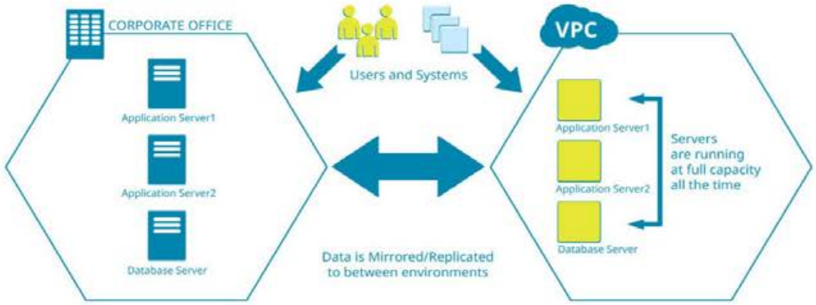
Option 3: Warm Standby

Taking the Pilot Light model one step further, warm standby creates an active/passive cluster. The minimum amount of capacity is provisioned in AWS. When needed, the environment rapidly scales up to meet full production demands. Companies receive (near) 100% uptime and (near) no downtime.



Option 4: Hot Standby

Hot standby is an active/active cluster with both cloud and on-premise components to it. Using weighted DNS load-balancing, IT determines how much application traffic to process in-house and on AWS. If a disaster or spike in load occurs, more or all of it can be routed to AWS with auto-scaling.



Important Assumptions (Example):

Current Backup / Disaster Recovery schema includes:

- Non-shared dedicated cloud (off-site) backup storage account
- Full imaging of daily/ weekly/monthly basis of all volumes and machines with 90-day history and retention (RPO history length can be changed)
- 3 daily recovery points of file based backups with 90-day retention and history (frequency can be changed).
- Local Storage Primary Backup and Disaster Recovery
- Cloud Storage Secondary Backup and Disaster Recovery
- Multi-AZ (Multi-Datacenter) replication of backup data and server images for remote cloud storage S3.
- Cross Region Replication of Data (to different regions for e.g. Ohio or California) is optional.

In the case of a Disaster Recovery event that requires the full restore of the operating ability of a single or multiple servers to **on-premise infrastructure:**

- Local Server Images will be used to restore sever availability.
- Files will be restored to last restore point from Local Storage.
- Recovery from an Operating System Failure or Application Error/Failure will by nature take longer than a simple restore of an image locally.
- The Purchasing Entity is responsible for providing working Virtual/Physical Machines Infrastructure that will host the restored server using Images or Snapshots.
- The process for a single server restore may take a few hours (range from 10 min – or more) due to an on-premise infrastructure issue given the capacity to restore on-premise is present.
- The process for a multiple server restores in total may take up to 5 hours or more (range from 30 min – or more) for restore due to an infrastructure issue or total disaster.

In the case of a Disaster Recovery event that requires the full restore of the operating ability of a single or multiple servers to **off-premise/remote site/AWS**:

- Server Images will be used to restore sever availability from Cloud Storage
- Files will be restored to last or safest restore point from Cloud Storage
- Recovery from an Operating System Failure or Application Error/Failure will by nature take longer than a simple restore of an image.
- The process for a single server restore may take a few hours (range from 10 min – more) within the same AWS region due to an on-premise infrastructure issue.
- The process for a multiple server restores in total may take several hours or more (range from 30 min – 4 hours or more) for restore to the same AWS region due to an on-premise infrastructure issue.

- In the event restores need to be made to a different AWS region, add additional hours for recovery time if cross region replication of images and data is not occurring. Otherwise it will be the same time frame as restore to the same AWS region.

Extended Downtime Scenario

If the root cause of the extended downtime is mutually agreed upon by i2m and Purchasing Entity to be the CSP (i.e. a host failure or unavailability of IaaS, SaaS, PaaS services) i2m will issue credit according to terms set in the SLA with the Purchasing Entity. The CSP in this case will be responsible for restoring availability of the service in a timely fashion that meets their own SLA further defined in this proposal. i2m strives to keep the Purchasing Entity informed of any information regarding the CSPs outage or downtime and relay that to the Purchasing Entity in a reasonable time.

If the i2m does not manage the solution then i2m is not responsible for the extended downtime but can assist the Purchasing Entity in any attempt to recover any systems/services. In the case of extended downtime, i2m will do its best effort to assist the entity in restoring critical production systems/services first specially ones that rely on high risk data or servers/services will be restored according to the priority set by the Purchasing Entity.

It is up to the Purchasing Entity to plan for Disaster Recovery and Business Continuity using their own methods/practices to avoid any service disruption. As services/solutions can be architected for minimal or zero impact to production services or systems. Extended downtime can be avoided or minimized by following AWSs Well-Architected Framework further mentioned in this proposal or by the use of another partner to formulate and execute a cloud DR Strategy for the Purchasing Entity.

If i2m manages the solution or service offering that has the extended downtime that was not caused by the CSP but by a fault in i2m’s solution/service (i.e. Value-Add service) i2m takes on responsibility of restoring operability of that solution/service in a timely fashion. Its insurance policy, if it applies, protects situations like this, and must be in effect to reimburse the Purchasing Entity of any damages caused by this downtime. i2m will issue credit according to terms set in the SLA with the Purchasing Entity if it applies. i2m will strive to ensure all the Purchasing Entity’s needs are met in a timely fashion. i2m’s solutions aim to avoid a scenario like this at all costs or at minimum plan to decrease the amount of downtime by geographic or data center isolation using different Regions and AZs on AWS. i2m’s solutions provide fail safes, redundancy and security with access controls to avoid scenarios like this. i2m’s cloud services auditing capabilities will help determine the root cause of the downtime. i2m will create a full report (a reason of incident report) with all of the evidence and documentation required by the Purchasing Entity to comply with any laws, rules and regulations it needs to abide by. i2m will comply with any reasonable requests made by the Purchasing Entity during this time. i2m will document it's failures and create a plan to remedy this gap in the Backup/Disaster Recovery or Management service plans across all of the Purchasing Entities Implementing our managed solution.

Purchasing Entity or CSPs Suffers an unrecoverable loss of data
If the root cause of the extended downtime is mutually agreed upon by i2m and Purchasing Entity to be the CSP (i.e. a host failure or data loss caused by IaaS, SaaS, PaaS services malfunction) i2m will issue credit according to terms set in the SLA with the Purchasing Entity, if it applies. The Purchasing Entity along with the CSP and i2m will take measures accordingly to remedy this either by using our Insurance Policies if it applies and/or through help from the CSP. i2m strives to keep the Purchasing Entity informed of any information regarding the CSPs outage or data loss and relay that to the Purchasing Entity in a reasonable time.

It is up to the Purchasing Entity to plan for Disaster Recovery and Business Continuity using their own methods/practices to avoid any data loss. As services/solutions can be architected for minimal or zero impact to production services or systems. Data loss can be avoided or minimized by following AWSs Well-Architected Framework further mentioned in this proposal or by the use of another partner to formulate and execute a cloud DR Strategy for the Purchasing Entity

If the data is managed by i2m (i.e. Disaster Recovery Plan (DRaaS) or Backup as a Service Plan (BaaS) is in place and managed by i2m)

i2m will determine the root cause and also if it is liable. The Purchasing Entity will also conduct its own investigation to determine who is at fault. i2m's insurance policy, which protects situations like this, must be in effect to reimburse the Purchasing Entity of any damages caused by this loss. i2m will strive to make sure all the Purchasing Entity needs are met in a timely fashion. i2m's solutions aim to avoid a scenario like this or at minimum plan to decrease the amount of data loss by geographic or data center data isolation using different Regions and AZs on AWS. i2m's solutions provide fail safes, redundancy and security with access controls to avoid scenarios like this. i2m's cloud services auditing capabilities will help determine the root cause of data loss. i2m will create a full report (a reason of incident report) with all of the evidence and documentation required by the Purchasing Entity to comply with any laws, rules and regulations it needs to abide by. i2m will comply with any reasonable requests made by the Purchasing Entity during this time. i2m will document it's failures and create a plan to remedy this gap in the Backup/Disaster Recovery service plans across all of the Purchasing Entities Implementing the solution that failed. i2m will issue credit according to terms set in the SLA with the Purchasing Entity if it applies.

If the data is not managed by i2m managed by the Purchasing Entity (where i2m has no access to data, data control mechanisms and does not manage a DRaaS or BaaS service). Then i2m is not be held responsible for this data loss. i2m can still assist the Purchasing Entity during this time.

CloudBerry and Druva Backup Onsite Physical Storage System specifications (optional, The Purchasing Entity may have on-premise storage available, or use storage infrastructure of choice)

Overview:

- i2m will deliver the Onsite Storage Device (NAS) and will assist The Purchasing Entity with Installation and Configuration remotely or on premise if requested (included)
- Disk Capacity ~48TB and expandable to ~96 TB (other models available with larger storage requirements)
- Device Manufacture and Make and Model:
  - BUFFALO TeraStation 51210RH Rackmount 12-Bay 48 TB (4TB x 12) RAID 2U Rack Mountable NAS & iSCSI Unified Storage - TS51210RH3204
- High speed up to 10GbE connection for the speeds of tomorrow
- Boot Authentication ensures the device is only accessible on authorized networks
- Third-party cloud integration
- Data replication protection and encryption
- i2m Warranty: 3 Year i2m warranty on the Physical Storage System, i2m to replace any failing hardware or disks within the 3 year term
- Manufacture Warranty: 3-year warranty includes HDD disk replacement
- Datasheet for Onsite Storage System Attached and available here: http://www.buffalotech.com/images/blog/TS5010_Series_Datasheet_-_English.pdf

CloudBerry Backup Features specifications

Overview:

- CloudBerry Backup supports backup and restore of virtual machines created and controlled by ESXi server which is a part of VMware vSphere product and support for Hyper-V servers.
- CloudBerry VM edition is designed to create, compress, encrypt and upload virtual machines backups to the cloud. The backup software connects directly to your cloud storage account and securely transfers backups to the cloud storage of your choice

Key Features

- VMware backup
  - CloudBerry supports backup and restore of virtual machines that created and controlled by ESXi server.
  - VMware level snapshots backups
- Hyper-V backup

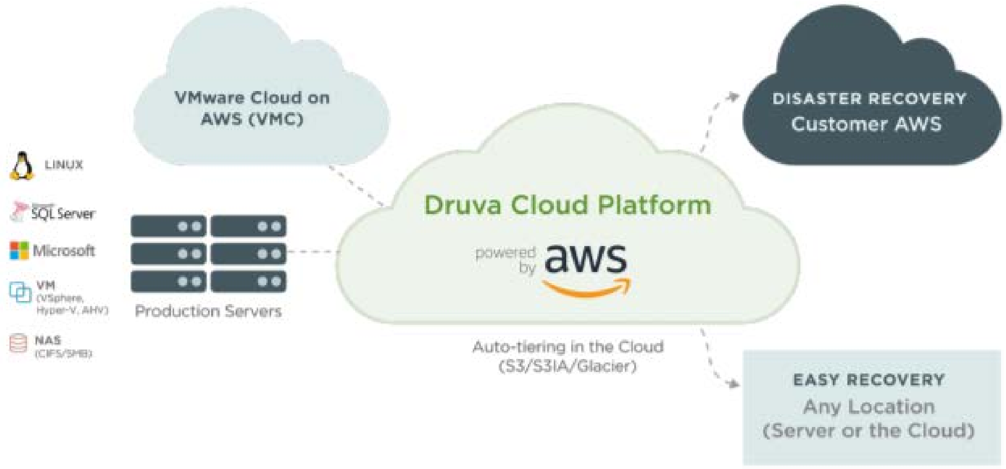
  - CloudBerry supports backup and restore of virtual machines that created and controlled by Hyper-V server.
- Image-Based backup and Bare-Metal restore:
  - Restore Servers as virtual machine to the cloud (Amazon EC2, Azure VM) or to physical servers or hosts
  - Doesn't require space on the local drive — back up to the cloud directly
  - Restores with USB Flash directly from the cloud
  - Backs up all or selected volumes
  - Restores to a dissimilar hardware
  - Restores to Hyper-V or VMware
  - File level restore from image based backup
- Exchange Server backup and restore
  - VSS-based backup of Microsoft Exchange Server
  - Mailbox-level restore for Exchange 2010 and above
- SQL Server backup and restore:
  - Full and differential backup
  - Transaction log backup
  - Predefined backup templates
  - Restore SQL Server databases and backup files
- Bare Metal and System State Backup
  - CloudBerry protects the system state itself, file system, system settings - entire server including applications and user data.
- Scheduling and Real-Time Backup
  - Setup hourly, daily, weekly, monthly backups or specify your own schedule. Real-Time backup allows to backup files and folders on Windows Server on change or creation.
- 256-bit AES Encryption
  - Encrypt backups with up to 256-bit strong keys on source side. All data sent to the cloud is also encrypted using the SSL protocols to protect while in transit.
- Compression
  - Reduce data overhead, decrease storage costs, aid bandwidth and accelerate backup completion with optional compression.
- Cloud and Local Backup
  - Backup to cloud storage of your choice or set up local backup if you want to send only a subset of your data to the cloud and keep the rest on your local backup storage.
- Block Level Backup
  - Backup only modified or new portions of files to add them to existing online data pool.
- C# API and Command Line Interface
  - Get backup plan statistics programmatically and use the Command Line

Interface to integrate backup with your own routines.

- Multiple Cloud Storage Support
  - Choose one of the supported public cloud storage, including: Amazon S3, Amazon Glacier, Windows Azure, Rackspace, OpenStack, Google Storage, HP Cloud, IBM SoftLayer (BlueMix) and many more.
- Network Locations Backup
  - Back up your network locations including network shares, NAS devices, mapped drives, etc.
- Cloud to Cloud Backup
  - Back up data from one cloud storage location to another. Use multiple cloud storage destinations to keep your cloud data backups.
- Cloud to Local Backup
  - Automate backup of the cloud data to local storage, external or network drive.
- Centralized Operations Management (Backup Solution Console)
  - Secure Web-Based Platform
  - MFA and username password combo for authentication
  - Single platform to manage/monitor all operations
  - Edit/Run/Restore backups from console
  - Notification options for success or failure of operations
  - Dashboard with real-time reporting that provides easy to analyze health check view for all backup plans
  - Report generation on operations, status, history, etc. (daily, weekly, annually)
- Email and Reporting Notifications
  - Set up customizable email and mobile notification feature to track each run of your backup and restore plans remotely and alert on critical jobs
- Purge
  - Set up Purge options to enable automated deletion of outdated data from your storage. Keep only latest versions of your backups.
- Backup Consistency Check
  - Monitor your backup consistency in cloud and local storage
- Supported Operating, Database and Email Systems:
  - Windows 7, 8, 8.1, 10
  - Windows Server 2003, 2008/R2, 2012/R2, 2016
  - Linux: Debian, Ubuntu 12/14/16, Suse 11/12, Red Hat 6.x/7.x, Fedora 12/21, CentOS 6/7, Oracle Linux 6.x/7.x
  - MS Exchange 2007/2010/2013/2016
  - SQL 2000, 2005, 2008, 2012, 2014, 2016 All editions in SQL Express Edition
  - mySQL support
  - MAC OSX all versions 10.8 or newer

Druva Pheonix Backup DR Features specifications

Druva Phoenix enables data protection and governance for enterprise infrastructure with a unique cloud–first approach, combining high performance, scalable backup, disaster recovery(DR), archival and analytics to simplify data protection, improve visibility and dramatically reduce the risk, cost and effort of managing today's complex information environment.


VMware Cloud on AWS (VMC)
LINUX
SQL Server
Microsoft
VM (VSphere, Hyper-V, AHV)
NAS (CIFS/SMB)
Production Servers
Druva Cloud Platform
powered by aws
DISASTER RECOVERY Customer AWS
Auto-tiering in the Cloud (S3/S3IA/Glacier)
EASY RECOVERY Any Location (Server or the Cloud)

Unified Backup, Archival, and DR in the Cloud

Phoenix enables cloud-based data protection and management for enterprise workloads including physical(file servers and/or NAS and databases), virtual(Microsoft Hyper-V, VMware vSphere, and Nutanix AHV) and hybrid(VMware Cloud on AWS (VMC)) environments. An IT team can easily failover virtual machines (VMs) for DR with a recovery time objective (RTO) of minutes and restore speeds up to 1 TB per hour, as well replicate data or spin up instances cross-region for test and dev(workload mobility) purposes—all on the same platform.

Significantly Lower TCO

With Druva Phoenix, you can achieve up to 60% lower total cost of ownership (TCO) than traditional or competitive solutions. Phoenix requires no additional hardware or software for data protection, utilizes global deduplication technology to deliver the smallest storage footprint, and offers customers a true "pay–as–you–go" model that eliminates wasted resources.

Cloud–Native SaaS Solution Built on AWS

Built from advanced cloud technologies and microservices in Amazon Web Services (AWS), Phoenix harnesses the native efficiencies and global reach of the public cloud while delivering unmatched storage flexibility, scalability, data durability, and security.

Accelerated Data Transfer to Meet Tight RTO and RPO Requirements

Phoenix leverages Druva's global, source–side deduplication technology to reduce bandwidth usage by up to 80% and ensures the smallest storage footprint—supercharging recovery point objectives(RPOs) and RTO. By combining forever incremental backups coupled with patented global deduplication, Druva Phoenix enables high-performance backups and restores. For tight RTO and RPO windows, the optional CloudCache feature breaks through RTO and RPO barriers by performing LAN speed restores at over 1 TB per hour.

Industry–Leading Data Security and Privacy

Druva’s approach to storing enterprise data utilizes both an advanced data–scrambling algorithm and a unique
envelope–based encryption model where the data and metadata are decoupled and encrypted. This guarantees that
your data is only accessible by you—a critical component to meeting today’s stringent global data privacy regulations. Under no circumstances can Druva access your data.

Key Features

Data Backup and Recovery

• Incremental Forever backup model
• Unlimited full restore points for quick recovery(no restore or cloud egress charges)
• Global, source–side, inline deduplication(Petabyte scale)
• Open file backup support
• (Optional) High-speed LAN backup and restore to local CloudCache for tight RTO/ RPO needs
• Restore speeds up to 1TB/hr

Administration

• Cloud-based centralized management
• Unified interface for hot, warm and cold backups
• Delegated administration model
• Backup scheduling and centralized policy management
• Bandwidth management

Disaster Recovery

• RTO within minutes of failover
• Configured VMs always in warm standby
• Secure failover to customer AWS VPC or VMC environment

Data Security and Privacy

• 256-bit AES encryption at rest
• 256-bit SSL encryption in transit
• SOC-2 Type II, HIPAA, Privacy Shield certification
• FedRAMP Certification
• No customer key management required
• Complete data privacy with no access to customer data—ever

Data Archiving

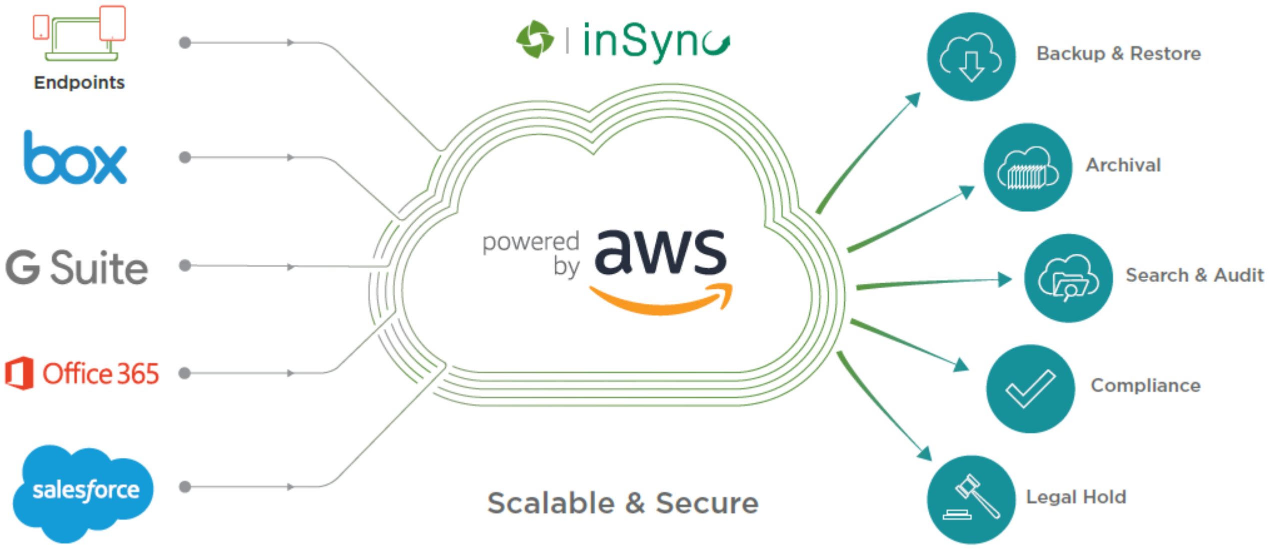
- Auto–tiered storage from hot or warm to long-term cold storage
- No limitation to the number of aged snapshots
- Shared global dedupe index for lower cost long–term storage

Scalable, Infinite Public Cloud

- Built on the leading public cloud—AWS (Amazon Web Services)
- SaaS–based pay-as-you elastic pricing model
- Consumption–based seamless scalability into the petabytes
- AWS GovCloud support

Druva InSync Endpoint Protection Backup Features specifications

Workforce mobility today is an essential part of any business, but it creates a number of challenges for IT. Data spreadacross devices and cloud services, unpredictable schedules, and varied network connections all complicate efforts to protect and govern enterprise information. With inSync, companies can protect their data stored in the cloud or on mobile devices while also addressing rising compliance and legal needs.



inSync provides a unified data protection and information governance solution that delivers a single pane of glass for viewing and managing dispersed data across endpoints and cloud applications—facilitating business continuity while not impacting employee productivity. inSync offers a single access point for viewing, monitoring and managing end-user data without having to manually access separate data sources through disparate solutions.

Ensure your data is protected without impacting user productivity

• Unified platform for endpoints and cloud applications to ensure data is protected across all user sources
• High performance, time-indexed snapshots with granular controls and scheduling for IT or end-users to restore files or return machines to their original state in the event of a successful ransomware intrusion
• Anytime, anywhere access from any device, with cross-platform support for smartphones and tablets—with additional support for IT-managed file sharing
• Immediate self-service restore empowers the end user to resume work on a new device quickly and seamlessly
• Automated installation and integrated mass deployment enable IT to quickly deploy inSync without user involvement
• Bandwidth throttling, resource usage and scheduling settings ensure maximum data protection with no user disruption

Maximize your data visibility and gain a proactive stance on risks
• Federated (metadata) search enables IT to quickly locate files across endpoints and cloud applications across all users, devices, and storage locations
• Unusual data activity monitors for abnormal file creations, updates, and deletions for the early detection and recovery against ransomware; Easily hit rewind by gaining insights into impacted data sets and the last known good snapshot
• Legal hold management enables data to be preserved, maintaining chain of custody until it's processed and analyzed in an eDiscovery platform
• Automated compliance monitoring and management enables IT to quickly identify and remediate potential data risks for organizations to address their data policy and compliance needs
• Extensive governance data policy configuration aids in segregating data regionally and meeting global data privacy requirements
• Integrated Data Loss Prevention (DLP) aids in preventing data breach of stolen or lost devices, including remote wipe (auto- or admin-initiated), geo-location, and enforced encryption

Engineered for performance with no compromise on security
• Cloud native architecture delivers real-time IO of data ensuring data is immediately accessible from any snapshot point, from any device
• Patented global deduplication delivers fast and efficient data collection by eliminating data redundancies across all users and from all their devices, resulting in up to 80% bandwidth savings
• WAN optimization, smart resource throttling, and auto-resume ensure that backups and restores are non-disruptive and complete efficiently for mobile users
• Enterprise-grade encryption in-transit (256-bit TLS) and at-rest (AES 256-bit) using digital envelope encryption ensuring the highest levels of data security and privacy

• Fully compliant cloud infrastructure, leveraging the power of Amazon Web Services (AWS) with Druva's own audits provides the highest level of security and protection for your data.

Implementation Process Goals

- Networking setup and configuration will begin with remote evaluation then on-site evaluation
  - Firewall and Network Configuration for all sites
  - Make sure all network connections to and from local and cloud storage adequate for backup operations and goals.

- Implementation of new local storage NAS(s) and cloud storage is non-disruptive to current environment:
  - Local Storage Device is installed on premise and configured.
  - Both VPC and S3 cloud infrastructure resources created using our custom Cloud Formation Stack Templates to avoid user prone errors in design
  - VPC has a IP-SEC VPN connection with The Purchasing Entity for Disaster Recovery of physical and virtual machines to the AWS cloud (remote site)
  - All existing on premise data required will be exported to AWS via use of AWS Snowball Device (a large 40/80TB NAS for Data Export to AWS)
  - All Data at Rest and during transmission will be encrypted with the AWS Snowball.
  - Device(s) will arrive onsite, i2m to configure and setup device for copying all data (live/archived) to the Snowball device
  - Once all Data has been captured, Snowball Device will be shipped to AWS to be imported to The Purchasing Entity's Cloud Storage AWS Account.
  - i2m to Sync Data Changes on daily basis via internet to cloud storage.
  - Data will be encrypted at rest and transfer to AWS for conversion into Data Volumes, Object Storage and Archived Object Storage respectively.
  - Folders/Files/Databases etc. directories marked for backup per machine or per network locations
  - Local Storage Reviewed for any permissions or backup accounts issues
  - Disaster Recovery of physical/virtual machines tested on critical machines for on-premise restores
  - Disaster Recovery of physical/virtual machines tested on a few critical machines for remote/off-site restores**
  - Any issues with backup source data will be addressed and resolved/excluded
  - Consistency Check of all data being backed up
  - Backup and Restore Plans/Jobs defined and tested
  - Backups are set to run on schedule for both local and cloud backup jobs
  - All-inclusive review/testing of entire backup environment
  - Full Project timeline and schedule attached dates will be moved accordingly see "Implementation Overview\Program Goals\Project Plan Time Line" folder

Security Considerations

- AWS Account Security Features:
  - Secure IT Access, All IT staff require MFA and username password (strict password policy) combo to do any work in the AWS Account.
  - IAM Security Features designed for user's least privileged access to services and i2m user accounts are defined and secured.
  - Any modification to AWS Resources or Configuration are tracked per i2m AWS Engineer/Architect (AWS Cloud Trail)
  - Root AWS Account locked by MFA (kept in secret) and very strict password policy. These Root Account credentials are to be held by executive IT Admins or Executive Staff, only requested by i2m if needed.
  - No client VPN or any other Remote Access methods to the VPC and Cloud and Storage Resources.

Training

- i2m to provide full training on the product:
  - Product Overview and Features
  - Creating Backup Plans/Jobs
  - Creating Restore Plans/Jobs
  - Retention and Archiving
  - Risk Management and Consistency Checking
  - Physical Storage Maintenance and Capacity Additions
  - Central Management Console Training
  - Reporting and Notification
  - Self-Service Portal restores for IT and authorized Staff
  - and more

Managed Solution

- i2m provides a managed solution
  - Daily Monitoring, Alerting, and assisted resolution
  - Backup failure and error assisted resolution
  - Assistance Creating Backup Plans/Jobs
  - Assistance Restore Plans/Jobs
  - Setting Retention and Archiving
  - General consulting and guidance around solution
  - Risk Management and Consistency Checking
  - Semi-Annual auditing of the backup solution
  - Remote Support and assisted resolution
  - Direct Support from Manufacturer CloudBerry and Druva Support
  - On-Site Support and Maintenance per customer request

- Physical Storage Maintenance and Capacity Additions
- Central Management Console setup and configuration
- Provide Reporting and Notification (daily, weekly, annually)
- Assistance in creating a DR plan during Implementation
- Assistance during DR scenarios per Customer Request

8.9 (E) DATA PROTECTION

8.9.1

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

Response:

Infrastructure as a Service (IaaS, PaaS, SaaS)
Amazon Web Services

- **Amazon S3**
  Amazon Simple Storage Services (Amazon S3) data protection. Protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

  Server-Side Encryption Amazon S3 can encrypt your data before saving it on disks in its data centers and decrypt it when the data is downloaded

  Server-side data encryption at-rest Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.

  You have three mutually exclusive options depending on how you choose to manage the encryption keys:

  Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) Each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. For more information, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) Similar to SSE-S3, but with some additional benefits along with some additional charges for using this service. There are separate permissions for the use of an envelope key (that is, a key that protects your data's encryption key) that provides added protection against unauthorized access of your objects in S3. SSE-KMS also provides you with an audit trail of when your key was used and by whom. Additionally, you have the option to create and manage encryption keys yourself, or use a default key that is unique to you, the service you're using, and the region you're working in. For more information, see Protecting Data Using Server-Side Encryption with AWS KMS–Managed Keys (SSE-KMS).

Use Server-Side Encryption with Customer-Provided Keys (SSE-C) – You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects. For more information, see Protecting Data Using Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).

Client-Side Encryption –Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, the consumer manages the encryption process, the encryption keys, and related tools.

- **Amazon EBS**
  Amazon Elastic Block Store (Amazon EBS) encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:

  - Data at rest inside the volume
  - All data moving between the volume and the instance
  - All snapshots created from the volume
  - All volumes created from those snapshots

  Amazon EBS encryption uses AWS Key Management Service (AWS KMS) customer master keys (CMKs) when creating encrypted volumes and any snapshots created from them. A unique AWS-managed CMK is created for you automatically in each region where you store AWS assets. This key is used for Amazon EBS encryption unless you specify a customer-managed CMK that you created separately using AWS KMS.

EBS encrypts your volume with a data key using the industry-standard AES-256 algorithm. Your data key is stored on-disk with your encrypted data, but not before EBS encrypts it with your CMK—it never appears there in plaintext. The same data key is shared by snapshots of the volume and any subsequent volumes created from those snapshots.

- **Amazon Identity Access Management (IAM)**

  AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

  Shared access to your AWS account

  You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.

  Granular permissions

  You can grant different permissions to different people for different resources. For example, you might allow some users complete access to Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift, and other AWS services. For other users, you can allow read-only access to just some S3 buckets, or permission to administer just some EC2 instances, or to access your billing information but nothing else.

  Secure access to AWS resources for applications that run on Amazon EC2

  You can use IAM features to securely provide credentials for applications that run on EC2 instances. These credentials provide permissions for your application to access other AWS resources. Examples include S3 buckets and DynamoDB tables.

  Multi-factor authentication (MFA)

  You can add two-factor authentication to your account and to individual users for extra security. With MFA you or your users must provide not only a password or access key to work with your account, but also a code from a specially configured device.

  Identity federation

  You can allow users who already have passwords elsewhere-for example, in your corporate network or with an internet identity provider-to get temporary access to your AWS account.

  Identity information for assurance

  If you use AWS CloudTrail, you receive log records that include information about those who made requests for resources in your account. That information is based on IAM identities.

PCI DSS Compliance
IAM supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS). For more information about PCI DSS, including how to request a copy of the AWS PCI Compliance Package, see PCI DSS Level 1.

For more detailed information, see the following AWS whitepapers:
https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

- **Amazon Elastic Map Reduce (Amazon EMR)**
  Beginning with Amazon EMR release version 4.8.0, you can use a security configuration to specify settings for encrypting data at-rest, data in-transit, or both. Each security configuration that you create is stored in Amazon EMR rather than in the cluster configuration, so you can easily reuse a configuration to specify data encryption settings whenever you create a cluster.

  Amazon S3 encryption works with EMR File System (EMRFS) objects read from and written to Amazon S3. You specify Amazon S3 server-side encryption (SSE) or client-side encryption (CSE) when you enable at-rest encryption. Amazon S3 SSE and CSE encryption with EMRFS are mutually exclusive; you can choose either but not both. Regardless of whether Amazon S3 encryption is enabled, Transport Layer Security (TLS) encrypts the EMRFS objects in-transit between Amazon EMR cluster nodes and Amazon S3. For in-depth information about Amazon S3 encryption, see Protecting Data Using Encryption in the Amazon Simple Storage Service Developer Guide.

  Amazon S3 Server-Side Encryption
  When you set up Amazon S3 server-side encryption, Amazon S3 encrypts data at the object level as it writes the data to disk and decrypts the data when it is accessed. For more information about SSE, see Protecting Data Using Server-Side Encryption in the Amazon Simple Storage Service Developer Guide.

  You can choose between two different key management systems when you specify SSE in Amazon EMR:

  - SSE-S3: Amazon S3 manages keys for you.
  - SSE-KMS: You use an AWS KMS customer master key (CMK) set up with policies suitable for Amazon EMR. For more information about key requirements for

Amazon EMR, see Using AWS KMS Customer Master Keys (CMKs) for Encryption. When you use AWS KMS, charges apply for the storage and use of encryption keys.

SSE with customer-provided keys (SSE-C) is not available for use with Amazon EMR.

Amazon S3 Client-Side Encryption

With Amazon S3 client-side encryption, the Amazon S3 encryption and decryption takes place in the EMRFS client on your cluster. Objects are encrypted before being uploaded to Amazon S3 and decrypted after they are downloaded. The provider you specify supplies the encryption key that the client uses. The client can use keys provided by AWS KMS (CSE-KMS) or a custom Java class that provides the client-side master key (CSE-C). The encryption specifics are slightly different between CSE-KMS and CSE-C, depending on the specified provider and the metadata of the object being decrypted or encrypted. For more information about these differences, see Protecting Data Using Client-Side Encryption in the Amazon Simple Storage Service Developer Guide.

Note

Amazon S3 CSE only ensures that EMRFS data exchanged with Amazon S3 is encrypted; not all data on cluster instance volumes is encrypted. Furthermore, because Hue does not use EMRFS, objects that the Hue S3 File Browser writes to Amazon S3 are not encrypted.

At-rest Encryption for Local Disks

Local disk encryption within a security configuration applies to instance store and EBS storage volumes in a cluster. It does not apply to EBS root device volumes. Beginning with Amazon EMR version 5.7.0, you can specify a custom AMI to encrypt the EBS root device volumes of EC2 instances. This is a separate setting from security configurations. For more information, see Using a Custom AMI in the Amazon EMR Management Guide.

Two mechanisms work together to encrypt storage volumes when you enable at-rest data encryption:

- **Open-source HDFS Encryption**: HDFS exchanges data between cluster instances during distributed processing, and also reads from and writes data to instance store volumes and the EBS volumes attached to instances. The following open-source Hadoop encryption options are activated when you enable local-disk encryption:
    - Secure Hadoop RPC is set to "Privacy", which uses Simple Authentication Security Layer (SASL).
    - Data encryption on HDFS block data transfer is set to true and is configured to use AES 256 encryption.

> **Note**
> You can activate additional Apache Hadoop encryption by enabling in-transit encryption (see In-Transit Data Encryption). These encryption settings do not activate HDFS transparent encryption, which you can configure manually. For more information, see Transparent Encryption in HDFS on Amazon EMR in the Amazon EMR Release Guide.

- **LUKS**. In addition to HDFS encryption, the Amazon EC2 instance store volumes and the attached Amazon EBS volumes of cluster instances are encrypted using LUKS. For more information about LUKS encryption, see the LUKS on-disk specification. At-rest encryption does not encrypt the EBS root device volume (boot volume). To encrypt the EBS root device volume, use Amazon EMR version 5.7.0 or later and specify a custom AMI. For more information, see Customizing an AMI in the Amazon EMR Management Guide.

  For your key provider, you can use an AWS KMS CMK set up with policies suitable for Amazon EMR, or a custom Java class that provides the encryption artifacts. When you use AWS KMS, charges apply for the storage and use of encryption keys. For more information, see AWS KMS Pricing.

In-Transit Data Encryption

Several encryption mechanisms are enabled with in-transit encryption. These are open-source features, are application-specific, and may vary by Amazon EMR release. The following application-specific encryption features can be enabled using security configurations:

- **Hadoop** (for more information, see Hadoop in Secure Mode in Apache Hadoop documentation):
  - Hadoop MapReduce Encrypted Shuffle uses TLS.
  - Secure Hadoop RPC is set to "Privacy" and uses SASL (activated in Amazon EMR when at-rest encryption is enabled).
  - Data encryption on HDFS block data transfer uses AES 256 (activated in Amazon EMR when at-rest encryption is enabled in the security configuration).

- **HBase:**
  - When Kerberos is enabled, the hbase.rpc.protection property is set to privacy for encrypted communication. For more information, see Client-side Configuration for Secure Operation in Apache HBase documentation. For more information about Kerberos with Amazon

EMR, see Use Kerberos Authentication.

- **Presto:**
    - Internal communication between Presto nodes uses SSL/TLS (Amazon EMR version 5.6.0 and later only).

- **Tez:**
    - Tez Shuffle Handler uses TLS (tez.runtime.ssl.enable).

- **Spark** (for more information, see Spark security settings):
    - Internal RPC communication between Spark components-for example, the block transfer service and the external shuffle service-is encrypted using the AES-256 cipher in Amazon EMR release version 5.9.0 and later. In earlier releases, internal RPC communication is encrypted using SASL with DIGEST-MD5 as the cipher.

    - HTTP protocol communication with user interfaces such as Spark History Server and HTTPS-enabled file servers is encrypted using Spark's SSL configuration. For more information, see SSL Configuration in Spark documentation.

You specify the encryption artifacts used for in-transit encryption in one of two ways: either by providing a zipped file of certificates that you upload to Amazon S3, or by referencing a custom Java class that provides encryption artifacts. For more information, see Providing Certificates for In-Transit Data Encryption with Amazon EMR Encryption.

- **Amazon Relational Database Service (Amazon RDS)**
  You can manage access to your Amazon RDS resources and your databases on a DB instance. The method you use to manage access depends on what type of task the user needs to perform with Amazon RDS:

  Run your DB instance in an Amazon Virtual Private Cloud (VPC) for the greatest possible network access control. For more information about creating a DB instance in a VPC, see Using Amazon RDS with Amazon Virtual Private Cloud (VPC).

  Use AWS Identity and Access Management (IAM) policies to assign permissions that determine who is allowed to manage RDS resources. For example, you can use IAM to determine who is allowed to create, describe, modify, and delete DB instances, tag resources, or modify DB security groups.

  Use security groups to control what IP addresses or Amazon EC2 instances can connect to your databases on a DB instance. When you first create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.

Use Secure Socket Layer (SSL) connections with DB instances running the MySQL, Amazon Aurora, MariaDB, PostgreSQL, Oracle, or Microsoft SQL Server database engines. For more information on using SSL with a DB instance, see Using SSL to Encrypt a Connection to a DB Instance.

Use RDS encryption to secure your RDS instances and snapshots at rest. Amazon RDS encrypted instances and snapshots use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS instance. Once your data is encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance. You don't need to modify your database client applications to use encryption.

Use network encryption and transparent data encryption with Oracle DB instances; for more information, see Oracle Native Network Encryption and Oracle Transparent Data Encryption

Use the security features of your DB engine to control who can log in to the databases on a DB instance, just as you do if the database was on your local network

- **Amazon Redshift**
  Amazon Redshift encrypts and keeps your data secure in transit and at rest using industry-standard encryption techniques. To keep data secure in transit, Amazon Redshift supports SSL-enabled connections between your client application and your Redshift data warehouse cluster. To keep your data secure at rest, Amazon Redshift encrypts each block using hardware-accelerated AES-256 as it is written to disk. This takes place at a low level in the I/O subsystem, which encrypts everything written to disk, including intermediate query results. The blocks are backed up as is, which means that backups are encrypted as well. By default, Amazon Redshift takes care of key management but you can choose to manage your keys using your own hardware security modules (HSMs) or manage your keys through AWS Key Management Service.

  Redshift Spectrum supports Amazon S3’s Server Side Encryption (SSE) using your account’s default key managed used by the AWS Key Management Service (KMS).

Software as a Service (SaaS)

Druva

All data that Druva sends to the cloud is protected while in flight using industry-standard Transport Layer Security (TLS). Once the data arrives in the Druva Cloud Service, it’s immediately encrypted using an AES 256-bit encryption key that is unique to, and completely controlled by, that customer. Druva has no access to this encryption key and as a result, has no access to any customer data. This unique one-to-one relationship of encryption key-to-customer guarantees that, in addition to the logical separation, there is an additional layer of access control that prevents data leakage in the cloud for data at rest. This customer encryption key is a session-only based key algorithm modeled on digital envelope encryption and results in the customer key never being stored, transferred or accessible from outside a user’s active cloud-side session. Thus, the need for expensive and complex key management solutions is eliminated. Yet another layer of security is applied, with Druva’s patented deduplication technology. Deduplication, or “dedupe,” refers to files being separated into individual blocks. Only unique blocks are sent to the service globally, across all devices. This means that entire files don’t have to be repeatedly stored and replaced when changes are made—just some of the building blocks. These unique blocks are stored in object-based storage without any identifying metadata, while block reference data and associated source file metadata are stored in a separate object-based NoSQL database.

This approach completely obfuscates the underlying data. Reconstitution of data is only possible through authenticated customer credentials, which are required to instantiate the session-based key mechanism. The result of this encryption of unique blocks is that the data is sharded, scrambled, and stored within the environment in a manner that makes it impossible for anyone to decrypt and reassemble the information without authenticated customer credentials.

Druva uses Encryption File System (EFS), a feature of Windows, to encrypt and decrypt data on your Windows laptops and implements a 256-bit AES encryption of files on your NTFS volumes to secure data at rest. EFS uses public key encryption in conjunction with symmetric key encryption to provide confidentiality for files that resists all but the most sophisticated methods of attack. The file encryption key (FEK) — a symmetric bulk encryption key — is used to encrypt the file and is then itself encrypted by using the public key taken from the user's certificate, which is located in the user's profile. The encrypted FEK is stored with the encrypted file and is unique to it. To decrypt the FEK, EFS uses the encryptor's private key which only the file encryptor has. Druva can only encrypt data that resides in the configured backup folders. Encryption and decryption are automated, with no additional steps or passwords needed. Backups continue to remain non-disruptive and transparent.

For more detailed information, see Druva Security Overview whitepaper: https://www.druva.com/documents/White-Paper_Druva-Security-Overview.pdf

Cloudberry

Client-Side Encryption

CloudBerry supports concurrent encryption during uploading to the cloud storage as well as the following symmetric key encryption algorithms. Our product supports the following encryption algorithms:

- AES-128
- AES-192
- AES-256

CloudBerry employs Microsoft's .NET API to use the aforementioned encryption algorithms. When encryption is enabled, the user is prompted to select an encryption algorithm and enter a password into the required text field. The password is subsequently converted into a cryptographic key and stored in the settings file and encrypted using the AES-128 algorithm.

Server-Side Encryption

Cloudberry also supports Amazon S3 Server-Side Encryption. All cloudberry backup data is either stored locally or in an Amazon S3 bucket. This enables us to use Amazon S3 Server-Side Encryption (SSE) on data in transit or at rest.

You have three mutually exclusive depending on how you choose to manage the encryption keys:

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) – Each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. For more information, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) – Similar to SSE-S3, but with some additional benefits along with some additional charges for using this service. There are separate permissions for the use of an envelope key (that is, a key that protects your data's encryption key) that provides added protection against unauthorized access of your objects in S3. SSE-KMS also provides you with an audit trail of when your key was used and by whom. Additionally, you have the option to create and manage encryption keys yourself, or use a default key that is unique to you, the service you're using, and the region you're working in. For more information, see Protecting Data Using Server-Side Encryption with AWS KMS–Managed Keys (SSE-KMS).

Use Server-Side Encryption with Customer-Provided Keys (SSE-C) – You manage the encryption keys and Amazon S3 manages the encryption, as it writes to disks, and decryption, when you access your objects. For more information, see Protecting Data Using Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).

Trend Micro

Trend Micro Worry-Free Services

Trend Micro Worry-Free Services is i2m's endpoint security solution for Windows, Mac, and mobile devices which is ideal for end-users. Worry-Free Business Security Services protects against viruses, ransomware, dangerous websites, and other threats. Real-time blocking in the cloud of latest threats before they reach your machines gives you peace of mind. Trend Micro Endpoint protections features include:

- Anti-malware
- Anti-Ransomware
- Evolving Threat Protection Using Machine Learning
- Behavior Analysis
- Device Control to limit access of USB drives and other attached devices to prevent data loss and block threats
- Firewall
- Application Control
- Advanced URL filtering to block inappropriate websites
- Web threat protection stops viruses and threats before they reach your business
- Data protection
- Automatic updates and patches pushed to users

Trend Micro Deep Security

Organizations are embracing the economic and operational benefits of cloud computing, turning to leading cloud providers including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and others. In the cloud, security is a shared responsibility. The cloud provider is responsible for the security of the physical and network infrastructure up to the hypervisor layer. It's up to you to protect what you put in the cloud-the workloads-including operating systems, service configuration, applications, and data.

Built on Trend Micro's industry-leading Hybrid Cloud Security solution, powered by XGen™, Trend Micro™ Deep Security™ as a Service is designed to augment cloud provider security with complete protection for cloud workloads. Deep Security provides a complete suite of security capabilities including intrusion detection and prevention, firewall, malware prevention with web reputation, predictive machine learning, sandbox analysis, integrity monitoring, log inspection, and multi-platform application control.

Deep Security as a Service gives you the proven protection of Deep Security without all the work. As a service deployment, we do the heavy lifting for you. We manage regular product and kernel updates, set up and maintain the security database, and administer the Deep Security manager.

Our cloud-based security offering enables quick setup and automates and simplifies security operations for cloud instances.

Cloudhealth

The CloudHealth policy engine is a powerful utility that enables you to define granular policies and automate them. Now, with CloudHealth Security Policies for AWS included in the policy engine, you can:

- Implement configurable policy-driven security alerts based on deep security best practice rules that are ranked according to severity.
- Flag policies for inclusion in the Policy Violation Report, which goes beyond simple alerting to provide deeper insight into the state of the violation, including affected resources and policy rule documentation.
- Define best practices across organizations, manage policy violations, automatically alert on critical issues, deliver violation reports via email, and suppress exempted resources.
- Provision fine-grained visibility using Perspectives that apply to specific business entities for service-level management, meaning that health checks can be customized for a particular business group.

DUO

Duo builds security into each step of our operations, including customer data handling, code release, upgrades, patch management, security policies and more.

We endeavor to meet compliance standards like PCI DSS, OWASP, ISO 27001, NIST 800 and more. A team of independent third-party auditors regularly audit and review our infrastructure and operations to ensure we’re secure enough to support our customers.

Duo’s two-factor solution is designed with security in mind. We use asymmetric cryptography, keeping only the public key on our servers and storing private keys on your users' devices in a tamper-proof secure element. Duo never stores your passwords - meaning your logins stay safe.

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.

Response:
i2m is willing to sign any relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

8.9.3

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

Response:
i2m confirms and attests it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. i2m shall not use the government data or government related data for any other purpose including but not limited to data mining. i2m or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP. Please also refer to our privacy policy stated above in section 8.5.2 and 8.5.3 for further clarification to this response.

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.

Response:
Our SLA is definitely negotiable to terms and conditions defined by the Purchasing Entity. The sample SLA provided by i2m in this RFP is just to show a baseline of a typical Service Level Agreement.

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.

Response:
AWS and all remaining SaaS Solutions offered have their own Service Level Agreements that are specified in section 8.4.1

Service Level Agreement
(Sample)

between

Include Information Management, Inc. DBA (i2m)
600 West Germantown Pike, Suite 400, Plymouth Meeting, PA 19462
&
NASPO ValuePoint Purchasing Entity
(Address)

This Agreement by and between Include Information Management, Inc. (known as i2m) and the NASPO ValuePoint Purchasing Entity (known as NVP), effective July 1st, 2018 is for services provided by i2m to NVP and defines the joint working relationship of the two parties.

1. DESCRIPTION OF SERVICES.
i2m will provide general IT Support Services (Services) which may include month-to-month maintenance fees for most aspects of the NVP computing environment such as network servers, workstations, security, Internet connectivity, network applications and cloud services. These services may include the deployment and use of the network management software for 7x24 hour systems monitoring services. See the "Statement of Work and Services" and "Cost Overview" sections of this document for a more detailed and specific description of the IT Services provided and fees.

2. LIMITATIONS OF SCOPE.
i2m will not be responsible for work that is beyond the scope of services set forth in this agreement. Either party may request changes to the defined services. Changes must be agreed to in writing and must reference and amend this Agreement. Any changes in the scope of services set forth in this agreement may require an adjustment in fees.

3. JOINT MANAGEMENT RESPONSIBILITY. Both parties share responsibility for work management and oversight. Designated managers from both parties will meet on a mutually defined regular basis to review business priorities and directions, key business milestones, work priorities, shared work assignments and approve completed work. Designated

managers from both parties will also be responsible for ensuring that high priority work is being addressed on a timely basis and that all key requirements are being met. Designated managers will be responsible for fully communicating issues and concerns and for ensuring that all team members are properly instructed on actions that need to be taken and corrections that need to be made. Designated managers will also be responsible for ensuring that agreed upon processes and work methods are being followed and that team members are appropriately aware of their responsibilities in carrying out their roles. Over and above these joint management responsibilities, NVP has full and exclusive responsibility for understanding and ensuring compliance with any regulatory, legal or contractual obligations related to data held by NVP (or by i2m on NVP’s behalf), information provided to customers and other third parties and safeguarding and security measures that may be required. i2m may participate in implementing needed systems services and functions, but NVP agrees that it shall be solely responsible for the final outcomes, actions taken and results produced, except to the extent of i2m’s negligence or intentionally wrongful acts.

4. PAYMENT FOR SERVICES.

NVP will pay monthly fees to i2m for Services rendered as described in the “Cost Overview” section of this document. Payment will be based on monthly invoices submitted by i2m to NVP and will be due and payable within twenty (20) days of the receipt of the invoice. Invoices will include fees for Fixed Rate and Recurring monthly services and Variable Rate fees for work that is provided on an hourly basis plus any direct costs such as supplies, printing, travel beyond what is directly involved in performing Services, and vendor charges incurred by i2m on NVP’s behalf. Any work that is over-and-above the agreed upon monthly fees shown in “Statement of Work and Services” will require prior approval from NVP before such fees are incurred. Invoices will be submitted at the beginning of the month for routine Services, and special project work that is over-and-above the planned monthly fees will be billed in the following monthly invoice. i2m reserves the right to assess and collect late-payment charges of one and one-half percent (1.5%) per month on undisputed past due balances. Any work performed by other parties that is coordinated by i2m will be billed directly to NVP by the 3rd party or, if previously agreed, will be passed on from i2m at cost.

5. PRICE ADJUSTMENT

i2m may make minor adjustments to products and costs defined in the “Statement of Work and Services” and “Cost Overview” sections of this document. These changes cannot exceed five percent of the total cost as defined in the “Statement of Work and Services” and “Cost Overview” sections of this document without written approval from NVP.

6. SERVICE HOURS.

Service price is based on the number of hours needed to manage the current number of PCs, Servers, Devices and Users and is contingent on the accuracy of this information. The services as described in the “Statement of Work and Services” are available 24x7. Quarterly or Biannual reviews may be needed to adjust the level of service due to the growth or other significant changes at NVP.

Normal Business Hours for i2m are from 8am to 5pm EST Monday-Friday. All other times are considered after-hours.

7. TERM/TERMINATION.

Except for reasons of non- performance by either party, this Agreement shall remain in effect for an initial period of twelve (12) months (the "Term") from the date of execution. . Either party may terminate this Agreement upon written notice for material breach, provided, however, that the terminating party has given the breaching party at least fourteen (14) days written notice of and the opportunity to cure such material breach. Termination for breach will not alter or affect the terminating party's right to exercise any other remedies for breach. Regardless of termination reason, client is responsible for any termination fees defined in Cost Overview" section of this document.

8. RENEWAL.

The parties may renew this agreement for additional one (1) year periods by mutual written agreement extending the term and providing specific reference to the new Term date, any modifications or replacements of the "Statement of Work and Services", and signatures from both parties. In the absence of a renewal agreement, this agreement can continue on a month-to-month basis beyond the term on mutual agreement, until terminated immediately upon written notice or renewed as defined in Section 8.

9. CONFIDENTIALITY.

i2m and its employees, agents, or representatives will not at any time or in any manner, either directly or indirectly, use for their personal benefit, or divulge, disclose, or communicate in any manner any information that is proprietary to NVP. i2m and its employees, agents, and representatives will protect such information and treat it as strictly confidential. This provision will continue to be effective after the termination of this Contract. NVP and its employees, agents, and representatives will protect and not divulge, disclose, or communicate in any manner any information that is proprietary to i2m, including, but not limited to, work methods, licensed software, management tools and forms, proposals, agreements, fees, billing rates, and any documents marked as confidential or proprietary. Upon termination of this Contract, i2m will return to NVP all records, notes, documentation and other items that were used, created, or controlled by i2m and which contain information proprietary to NVP. NVP will return to i2m all records, notes, documentation, licensed software and other items that were used, created, or controlled by NVP and which contain information proprietary to i2m. The foregoing obligations shall not apply where a party is required by NVP to disclose such information.

10. WARRANTY.

i2m shall provide its services and meet its obligations under this Agreement in a timely and professional manner, using knowledge and skills consistent with generally acceptable and prevailing industry standards for an IT service provider.

11. LIMITATIONS OF LIABILITY.

Except to the extent resulting from the negligence or intentional misconduct of i2m, i2m's liability to pay damages for any losses incurred by NVP as a result of breach of contract by i2m, regardless of the theory of liability asserted, is limited to no more than the total amount of the annual base fee paid under this Agreement. In any case, i2m and its licensees will not be liable for lost profits or any consequential, indirect, punitive, exemplary or special damages. In addition, except to the extent of i2m’s negligence or intentional misconduct, i2m shall have no liability to NVP arising from or relating to any third party hardware, software, information or materials. i2m is also not liable for direct or indirect damages created by viruses, hackers or other malicious or accidental destruction of systems or data, except to the extent of i2m’s negligence or intentional misconduct , though i2m will make every reasonable effort to prevent or minimize exposure to such risks.

12. ENTIRE AGREEMENT.

This Agreement plus any Appendices and sections of this document and future letters specifically referencing and amending this Agreement contains the entire agreement of the parties, and there are no other promises or conditions in any other agreement whether oral or written concerning the subject matter hereunder. This Contract supersedes any prior written or oral agreements between the parties.

13. SEVERABILITY.

If any provision of this Agreement will be held to be invalid or unenforceable for any reason, the remaining provisions will continue to be valid and enforceable. If a court finds that any provision of this Agreement is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision will be deemed to be written, construed, and enforced as so limited.

14. SUCCESSORS AND ASSIGNS.

The provisions of this Agreement shall be binding upon and inure to the benefit of the heirs, personal representatives, successors and assigns of the parties.

15. INDEPENDENT BUSINESSES.

Both parties acknowledge that i2m is an independent contractor and is not an agent, partner, joint venture nor employee of NVP. i2m shall only have authority to bind or otherwise obligate NVP if agreed in writing by both parties. NVP shall only have authority to bind or otherwise obligate i2m if agreed in writing by both parties. In all other cases neither party shall have authority to bind or otherwise obligate the other in any manner nor shall either party represent that it has a right to do so.

16. INDEMNIFICATION.
Each party will defend, indemnify and hold the other party harmless against any claims by third parties, including all costs, expenses and reasonable attorneys' fees, arising out of or in conjunction with such party's performance under or breach of this Agreement. In addition, i2m represents and warrants that any software or programs designed by i2m as IT Services shall be an original creation and that such software or programs shall not be copied from, and shall not infringe, any rights of any third parties. i2m will defend, indemnify and hold NVP harmless against any claims by third parties, including all costs, expenses and attorneys' fees, arising out of or in conjunction with any breach by i2m of its representation in the preceding sentence.

17. NOTICES. (a) FROM US. Except as otherwise provided herein, notices we send to you under this Agreement must be sent by email to the email address on record with i2m at the time of this Agreement. . You are responsible for keeping your email address current and accurate at all times and notifying i2m of any changes. Any notice we send to the then-current email address on record will be deemed to be received when it is sent even if you do not actually receive it. (b) FROM YOU. Except as otherwise provided herein, notices you send to us under this Agreement must be in writing and sent at your own cost either (i) by email to billing@include-im.com; or (ii) by certified mail, return receipt requested, or nationally recognized courier (e.g., FedEx or U.P.S.) with a signature required to the following address: Include Information Management, Inc., 600 West Germantown Pike, Suite 400, Plymouth Meeting, PA 19462.
(c) WHEN EFFECTIVE. A notice under this Agreement is effective when received. An email notice under this Agreement will be deemed received when sent. All other notices will be deemed received when signed for as indicated by the signed delivery receipt.

18. RELATION OF PARTIES.
The performance by i2m of its duties and obligations under this Agreement will be that of an independent contractor, and nothing herein will create or imply an agency relationship between i2m and NVP, nor will this Agreement be deemed to constitute a joint venture or partnership between the parties.

19. EMPLOYEE SOLICITATION/HIRING.
During the period of this Agreement and for twenty-four (24) months thereafter, neither party will directly or indirectly solicit or offer employment to or hire any employee, former employee, subcontractor, or former subcontractor of the other. The terms "former employee" and "former subcontractor" will include only those employees or subcontractors of either party who were employed or utilized by that party on the Effective Date of this Agreement.

20. ASSIGNMENT; RESALE; BINDING EFFECT.

You may not assign this Agreement or resell the right to use the i2m Cloud Services without our prior written consent. We may assign this Agreement at any time. This Agreement will be binding upon and inure to the benefit of all of our and your successors and assigns, who will be bound by all of the obligations of their predecessors or assignors.

21 ARBITRATION.

Any dispute arising under this Agreement will be subject to binding arbitration by a single Arbitrator with the American Arbitration Association (AAA), in accordance with its relevant industry rules, if any. The parties agree that this Agreement will be governed by and construed and interpreted in accordance with the laws of the State of Pennsylvania. The arbitration will be held in Pennsylvania. The Arbitrator will have the authority to grant injunctive relief and specific performance to enforce the terms of this Agreement. Judgment on any award rendered by the Arbitrator may be entered in any Court of competent jurisdiction.

22. ATTORNEYS FEES

If any litigation or arbitration is necessary to enforce the terms of this Agreement, the prevailing party will be entitled to recover reasonable attorneys' fees and costs from the other party.

23. INSURANCE.

i2m shall acquire and maintain at its sole cost and expense; (i) Statutory Worker's Compensation Insurance and Employer's Liability Insurance, (ii) risk coverage of not less than ten million dollars ($10,000,000) for physical loss or damage, and (iii) Bodily Injury and Property Damage (iv) Privacy/Cyber Security, Errors and Omissions Insurance with a combined single limit of not less than ten million dollars ($10,000,000).

24. NEUTRAL INTERPRETATION.

This Agreement will be construed and interpreted in a neutral manner. No rule of construction or interpretation will apply against either you or us.

25. i2m CLOUD SERVICES

1. PROVIDERS. i2m Cloud Services is a managed cloud service that utilizes several commercially available cloud infrastructures that may include Amazon Web Services, Linode, HP Cloud Services, Azure Cloud Computing (Microsoft), IBM, and Google Cloud Platform

2. REPRESENTATIONS. You represent and warrant to us that (i) the information you provide in connection with your use of i2m Cloud Services is accurate and complete; (ii) no Content on the Cloud Servers is illegal, defamatory, malicious, harmful, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation, or age;(iii) you

accurately and adequately disclose how you collect and treat data collected from visitors to any Website or users of any Application on the Cloud Servers; (iv) your use of the Cloud Services will comply with all applicable laws, rules and regulations; (v) you will not attempt to circumvent or disable any of the security-related, management, or administrative features of the Cloud Services; (vi) you have obtained all consents and licenses required for both of us to legally access and use all software you place on the Cloud Servers without infringing any ownership or intellectual property rights; (vii) the execution and delivery of this Agreement will not conflict with or violate any provision of your charter, by-laws or other governing documents; and (viii) you have otherwise taken all necessary steps to legally execute this Agreement.

3. HIGH RISK USE. You may not use the i2m Cloud Services for any application where a failure of those Cloud Services could result in death, serious injury, environmental damage or property damage. Examples of prohibited uses include medical life support devices, water treatment facilities, nuclear facilities, weapons systems, chemical facilities, mass transportation, aviation and flammable environments. You acknowledge that we make no assurances that the Cloud Services are suitable for any high-risk use.

4. MAINTENANCE; SERVICE MODIFICATIONS AND DISCONTINUANCE. In addition to our right to suspend or terminate the i2m Cloud Services in accordance with Section 4, we may suspend all or part of i2m Cloud Services without liability or prior notice to you (i) in order to maintain (i.e., modify, upgrade, patch, or repair) our Infrastructure or any Cloud Servers; (ii) as we determine may be required by NVP or regulation; or (iii) as we determine to be necessary to protect our Infrastructure and clients from unauthorized access or an attack on the Cloud Services. Notwithstanding the foregoing, we will endeavor in good faith to provide you with advance notice of any suspension or termination under this Section 24.4 in accordance with the notice provisions in Section 16 and we will provide you with notice of the suspension or termination as soon as it becomes practicable for us to do so.

5. SERVICE LEVEL AGREEMENT. When we use the term “Service Level Agreement” or “SLA” anywhere in this Agreement, we are referring to the service level agreement set forth in this Section 24.5. We will use commercially reasonable efforts to make i2m Cloud Services available 99.95% of the Service Year. ”Service Year” means the three hundred sixty five-day period immediately preceding a claim for a service credit. (a) SERVICE CREDIT. Uptime for each Service Year will be calculated by subtracting from 100% the percentage of time during which our Infrastructure was unavailable to all of our Cloud Service clients (the “Uptime Percentage”). If the Uptime Percentage for the Service Year is less than 99.95%, you will be eligible for a service credit equal to 10% of your i2m Cloud Services bill for the calendar month in which the Uptime Percentage dropped below 99.95%. The Uptime Percentage will be calculated using five-minute increments. (b) DOWNTIME EXCLUSIONS. Downtime does not include unavailability caused by one or more of the following: (i) maintenance, a suspension, or a termination of the i2m Cloud Services; (ii) the failure of servers or services outside of a datacenter on which the i2m Cloud Services are dependent, including, but not limited to, inaccessibility on the Internet that is not caused by the Cloud Server host

datacenter infrastructure or network providers; (iii) a force majeure event such as an act of God, act of war, act of terrorism, fire, governmental action, labor dispute, and any other circumstances or events not in our direct control; (iv) an attack on host datacenter infrastructure, including a denial of service attack or unauthorized access (i.e., hacking); (v) unavailability not reported by you in accordance with the reporting provisions in Section 24.5(c) within five (5) of the days of the date on which the Uptime Percentage dropped below 99.95%; (vi) your use of a separate i2m service that is not subject to this SLA; (vii) unavailability that results from the failure of individual Cloud Servers and that is not attributable to an event causing unavailability to all clients using the i2m Cloud Services; or (viii) unavailability that is caused by your breach of this Agreement. (c) SERVICE
6. CREDIT PROCEDURES. We will determine, in our reasonable discretion, your eligibility for service credits and the amount of service credits awarded pursuant to this SLA. To be eligible for service credits, you must send us a reasonably detailed, written request for service credits no later than five (5) Business Days after the day on which your Uptime Percentage first drops below 99.95%. To be deemed valid, your request must include (i) the dates and times of each period of Cloud Service unavailability upon which your request is based; (ii) the instance names of the affected Cloud Servers; and (iii) a description of any events from the Cloud Services portal that may have indicated a system-wide unavailability during the stated dates and times. If your Uptime Percentage is confirmed by us to be less than 99.95% for the Service Year, we will issue a service credit during the billing cycle following the month in which we determine that you are eligible for one. All service credits will be applied to fees due from you to us for Cloud Services; we will not pay any service credit to you as a refund. If you fail to provide us with a valid request, you will not be eligible for a service credit. Our calculation of your Uptime Percentage and all service credits will be based on our records and data. Any dates and times that you previously reported that led to a successful service credit claim cannot be used for future claims. (d) LIMITATION. THE SERVICE CREDITS DESCRIBED IN THIS SLA ARE YOUR SOLE AND EXCLUSIVE REMEDY FOR THE UNAVAILABILITY OF A CLOUD SERVER OR CLOUD SERVICE.

26. FORCE MAJEURE.
If the performance of any part of this Agreement, other than the payment of money, is prevented or delayed by reason of an act of God, act of war, act of terrorism, fire, governmental action, labor dispute or other cause beyond the performing party’s control, then that party will be excused from performance for the length of that prevention or delay.

Acceptance of Master Services Agreement and its Terms and Conditions

The above prices, specifications, and conditions are satisfactory and hereby accepted. Include Information Management, Inc. is authorized to do this work and supply these materials and services as specified.

8.11 (E) DATA DISPOSAL

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

Response:

Please refer to section 8.5.1 and 8.7.1 for detailed response to this section.

i2m inherits AWS Storage Device Decommissioning procedures and policies when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer 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

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.

Response:

i2m inherits the SLA of the cloud solution offerings in this proposal further defined in section 8.4.1

i2m's SLA Policies and Procedures:

SERVICE LEVEL AGREEMENT

When we use the term "Service Level Agreement" or "SLA" anywhere in this Agreement, we are referring to the service level agreement set forth in this Section 24.5. of our contract. We will use commercially reasonable efforts to make i2m Cloud Services available 99.95% of the Service Year. "Service Year" means the three hundred sixty five-day period immediately preceding a claim for a service credit. (a) SERVICE CREDIT. Uptime for each Service Year will be calculated by subtracting from 100% the percentage of time during which our Infrastructure was unavailable to all of our Cloud Service clients (the "Uptime Percentage"). If the Uptime Percentage for the Service Year is less than 99.95%, you will be eligible for a service credit equal to 10% of your i2m Cloud Services bill for the calendar month in which the Uptime Percentage dropped below 99.95%. The Uptime Percentage will be calculated using five-minute increments. (b) DOWNTIME EXCLUSIONS. Downtime does not include unavailability caused by one or more of the following: (i) maintenance, a suspension, or a termination of the i2m Cloud Services; (ii) the failure of servers or services outside of a datacenter on which the i2m Cloud Services are dependent, including, but not limited to, inaccessibility on the Internet that is not caused by the Cloud Server host datacenter infrastructure or network providers; (iii) a force majeure event such as an act of God, act of war, act of terrorism, fire, governmental action, labor dispute, and any other circumstances or events not in our direct control; (iv) an attack on host datacenter infrastructure, including a denial of service attack or unauthorized access (i.e., hacking); (v) unavailability not reported by you in accordance with the reporting provisions in Section 24.5(c) within five (5) of the days of the date on which the Uptime Percentage dropped below 99.95%; (vi) your use of a separate i2m service that is not subject to this SLA; (vii) unavailability that results from the failure of individual Cloud Servers and that is not attributable to an event causing unavailability to all clients using the i2m Cloud Services; or (viii) unavailability that is caused by your breach of this Agreement. (c) SERVICE

CREDIT PROCEDURES
We will determine, in our reasonable discretion, your eligibility for service credits and the amount of service credits awarded pursuant to this SLA. To be eligible for service credits, you must send us a reasonably detailed, written request for service credits no later than five (5) Business Days after the day on which your Uptime Percentage first drops below 99.95%. To be deemed valid, your request must include (i) the dates and times of each period of Cloud Service unavailability upon which your request is based; (ii) the instance names of the affected Cloud Servers; and (iii) a description of any events from the Cloud Services portal that may have indicated a system-wide unavailability during the stated dates and times. If your Uptime Percentage is confirmed by us to be less than 99.95% for the Service Year, we will issue a service credit during the billing cycle following the month in which we determine that you are eligible for one. All service credits will be applied to fees due from you to us for Cloud Services; we will not pay any service credit to you as a refund. If you fail to provide us with a valid request, you will not be eligible for a service credit. Our calculation of your Uptime Percentage and all service credits will be based on our records and data. Any dates and times that you previously reported that led to a successful service credit claim cannot be used for future claims. (d) LIMITATION. THE SERVICE CREDITS DESCRIBED IN THIS SLA ARE YOUR SOLE AND EXCLUSIVE REMEDY FOR THE UNAVAILABILITY OF A CLOUD SERVER OR CLOUD SERVICE.

8.12.2

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

Response:
%99.95

See detailed response for section 8.12.1

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.

Response:
Support Services from i2m NASPO ValuePoint Purchasing Entities:

Pre/Post project or service delivery implementations NASPO ValuePoint and its Purchasing Entities shall send any request for any products/services support, general questions and additional account creation requests to support@i2m.cloud. Please preface any requests that are an Emergency or Urgent as mentioned in emergency or rush services section in this proposal. Purchasing Entity can call our direct support number at 1-888-991-3814 and choose 2 for cloud services support.

Email should have subject line "NASPO ValuePoint – Support Request – The Purchasing Entities Legal Business Name – Short Description of Issue"

In the body of the request please include in detail the nature of your request, the products/services you need assistance with and primary point of contact if different from the requester.

i2m will respond to the email to either schedule a meeting to further discuss, or reply to the request directly via email. A Virtual/Audio Conference details will be sent to the Purchasing Entity if meeting/call is re-quested. It is encouraged that the Purchasing Entity include in the meeting/call any relevant staff members that will be delivering/implementing the requested cloud solution to the organization.

Who will be responding to support requests is detailed in the section 7 "Organization and Staffing" of this proposal.

Availability will be up to the Purchasing Entity to decide. i2m can meet any support needs 24/7.

8.12.4

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

Response:
Please see response to section 8.12.1 answers this response in detail.

8.12.5

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

Response:
Amazon Web Services
For AWS accounts managed by i2m, we will notify the Purchasing Entity of any impending maintenance or any event that may affect operational availability of production environments in AWS. Examples include cloud service provider notifying i2m of service degradation, service unavailability, or service termination. For accounts managed by the Purchasing Entity, alerts can be configured to send directly to email or viewed from the AWS management console.

AWS can schedule events for your instances, such as a reboot, stop/start, or retirement. These events do not occur frequently. If one of your instances will be affected by a scheduled event, AWS sends an email to the email address that's associated with your AWS account prior to the scheduled event, with details about the event, including the start and end date. Depending on the event, you might be able to take action to control the timing of the event.

SaaS Solutions (DUO, Trend Micro, Druva, CloudBerry, CloudHealth)
i2m will notify the Purchasing Entity of any impending maintenance or any event that may affect operational availability of SaaS solutions offered. Examples include SaaS service provider notifying i2m of service degradation, service unavailability, or service termination.

8.12.6

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

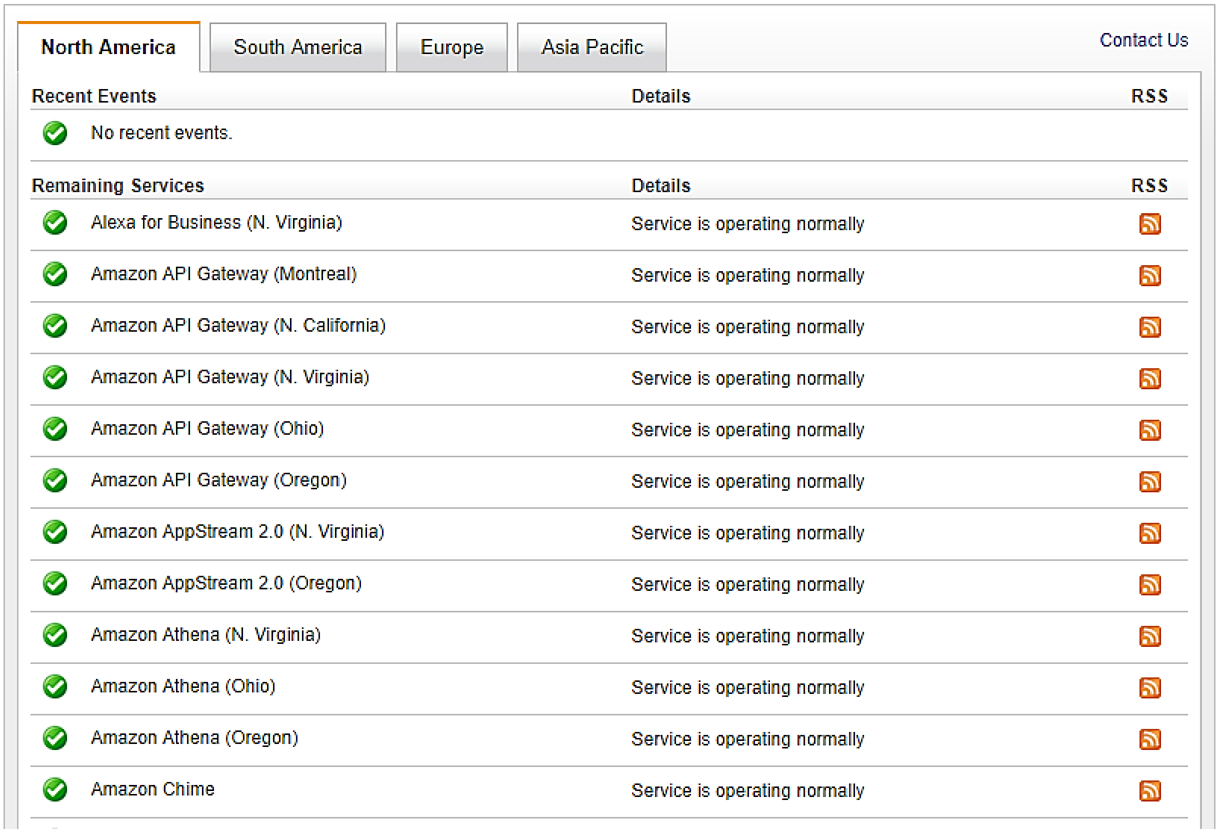
Response:
Please see response to section 8.12.1 answers this response in detail. When Disaster Recovery metrics are not met the same policies apply as section 8.12.1.

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.

Response:
Amazon Web Services

- **AWS Service Health Dashboard**
  https://status.aws.amazon.com/
  Amazon Web Services publishes up-to-the-minute information on service availability. The Service Health Dashboard is available over the web and provide real-time statistics.



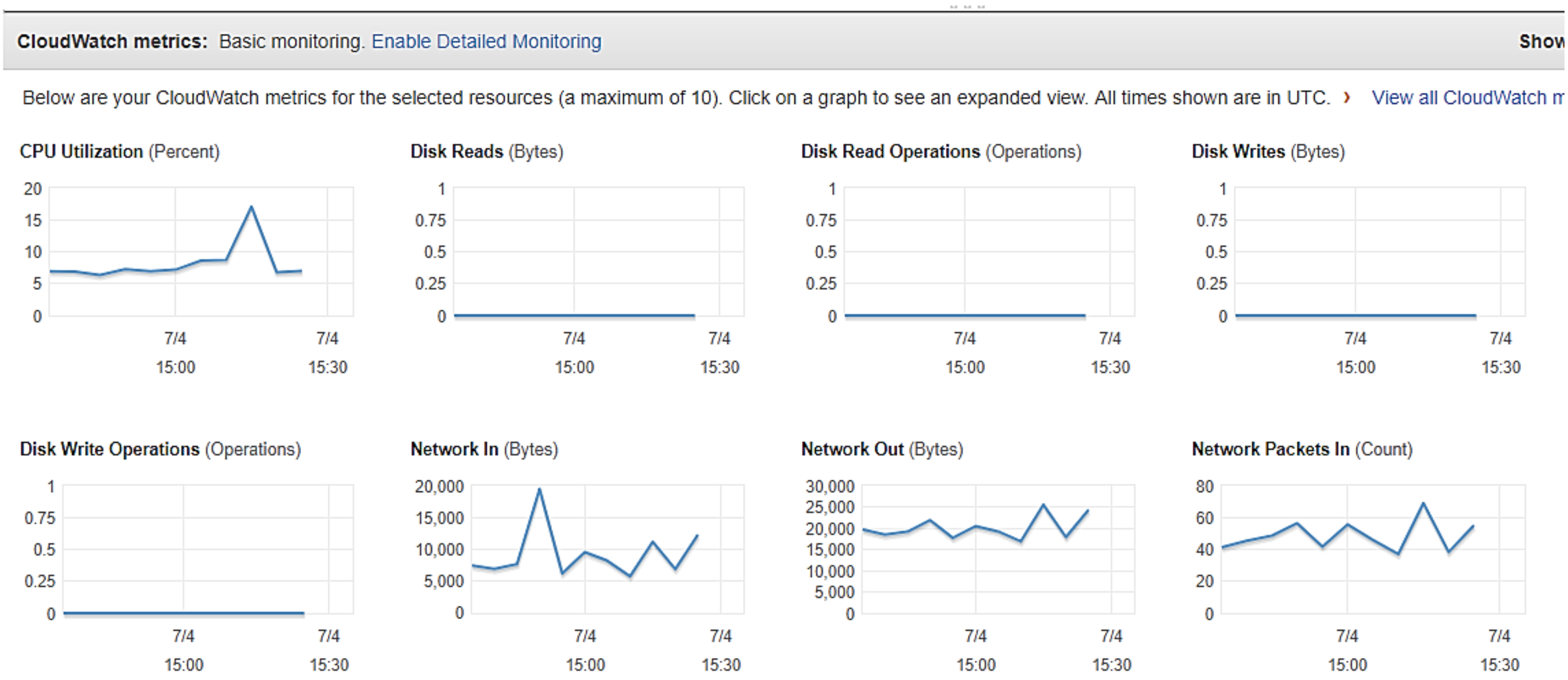
	Recent Events	Details	RSS
✓	No recent events.		

	Remaining Services	Details	RSS
✓	Alexa for Business (N. Virginia)	Service is operating normally	
✓	Amazon API Gateway (Montreal)	Service is operating normally	
✓	Amazon API Gateway (N. California)	Service is operating normally	
✓	Amazon API Gateway (N. Virginia)	Service is operating normally	
✓	Amazon API Gateway (Ohio)	Service is operating normally	
✓	Amazon API Gateway (Oregon)	Service is operating normally	
✓	Amazon AppStream 2.0 (N. Virginia)	Service is operating normally	
✓	Amazon AppStream 2.0 (Oregon)	Service is operating normally	
✓	Amazon Athena (N. Virginia)	Service is operating normally	
✓	Amazon Athena (Ohio)	Service is operating normally	
✓	Amazon Athena (Oregon)	Service is operating normally	
✓	Amazon Chime	Service is operating normally	

- **AWS CloudWatch**
  AWS CloudWatch Metrics are data about the performance of your systems. By default, several services provide free metrics for resources (such as Amazon EC2 instances, Amazon EBS volumes, and Amazon RDS DB instances). You can also enable detailed monitoring some resources, such as your Amazon EC2 instances, or publish your own application metrics. Amazon CloudWatch can load all the metrics in your account (both AWS resource metrics and application metrics that you provide) for search, graphing, and alarms.

  Metric data is kept for a period of 15 months, enabling you to view both up-to-the-minute data and historical data. You can view your data at different granularities. For example, you can choose a detailed view (for example 1 minute), which can be useful when troubleshooting. You can choose a less detailed view (for example, 1 hour), which can be useful when viewing a broader time range (for example, 3 days) so that you can see trends over time.

  AWS CloudWatch reports are available over the web through your AWS Management Console.



CloudWatch metrics: Basic monitoring. Enable Detailed Monitoring

Below are your CloudWatch metrics for the selected resources (a maximum of 10). Click on a graph to see an expanded view. All times shown are in UTC. › View all CloudWatch m

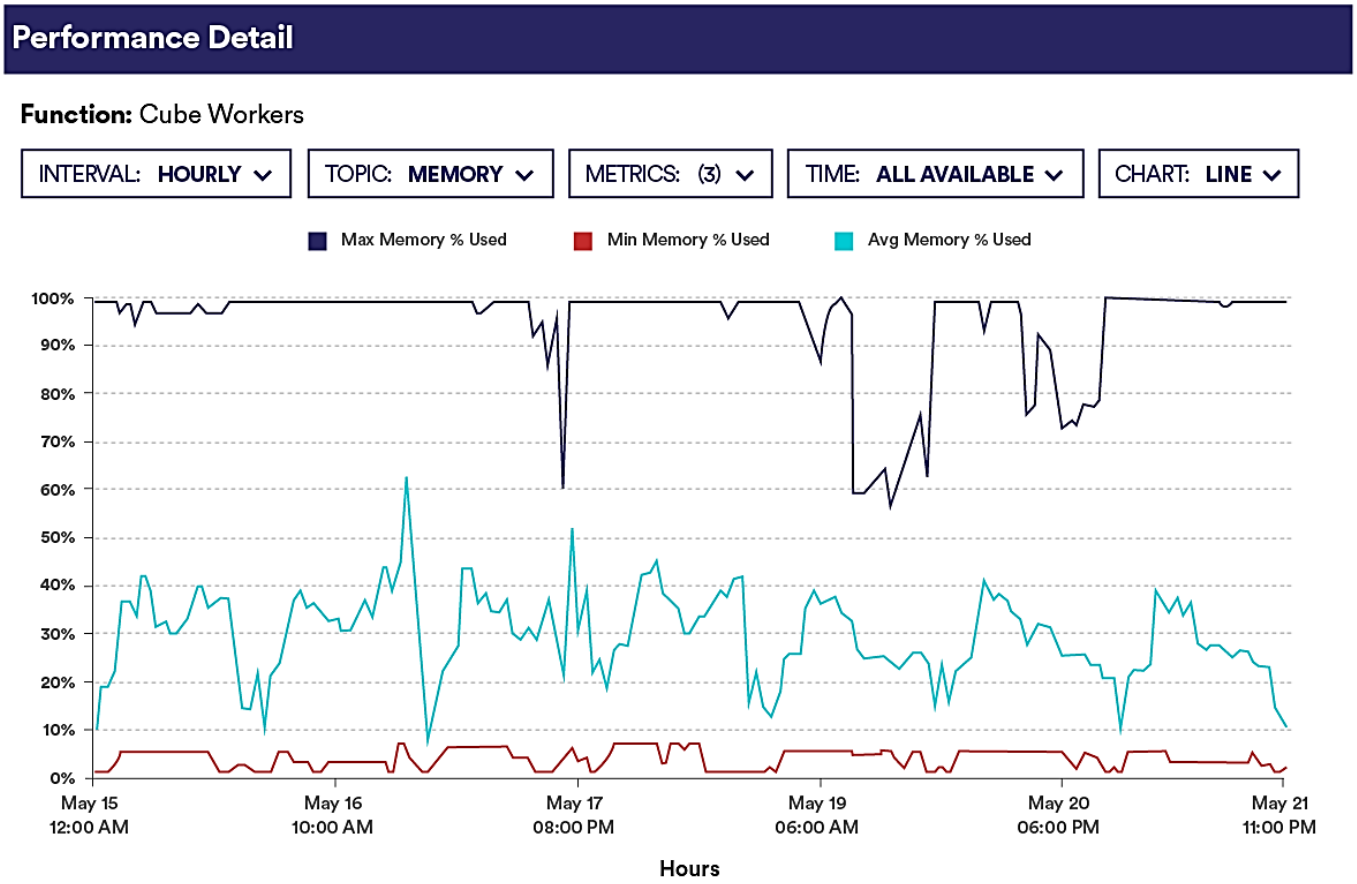
CloudHealth

CloudHealth enhances user visibility and control of cloud costs, usage, security, and performance. The heightened transparency across any multi-cloud environment drives more informed decision making. Correlate data for analysis and reporting against business objectives. With CloudHealth you can create interactive reports across multiple dimensions, time frames, Perspectives, Groups, or any combination of these.

CloudHealth interactive reports evaluate hybrid infrastructure events and trends. They can help you forecast for improved cost, availability, and performance optimization. To truly understand asset performance and utilization, you must collect, trend and report on both a granular and a macro level across CPU, memory, network, disk, IOPS, throughput, and more. CloudHealth ingests this data from disparate sources to correlate, analyze, and visualize it. Evaluate your cloud infrastructure based on application, workload, and environment to better understand resource utilization and optimize performance.

CloudHealth reports are completely customizable and are available to view in near real-time over the web. Reports can also be emailed or downloaded locally depending on preference. Since CloudHealth continuously pulls data from any of your cloud data sources, the information in the platform is always up-to-date.

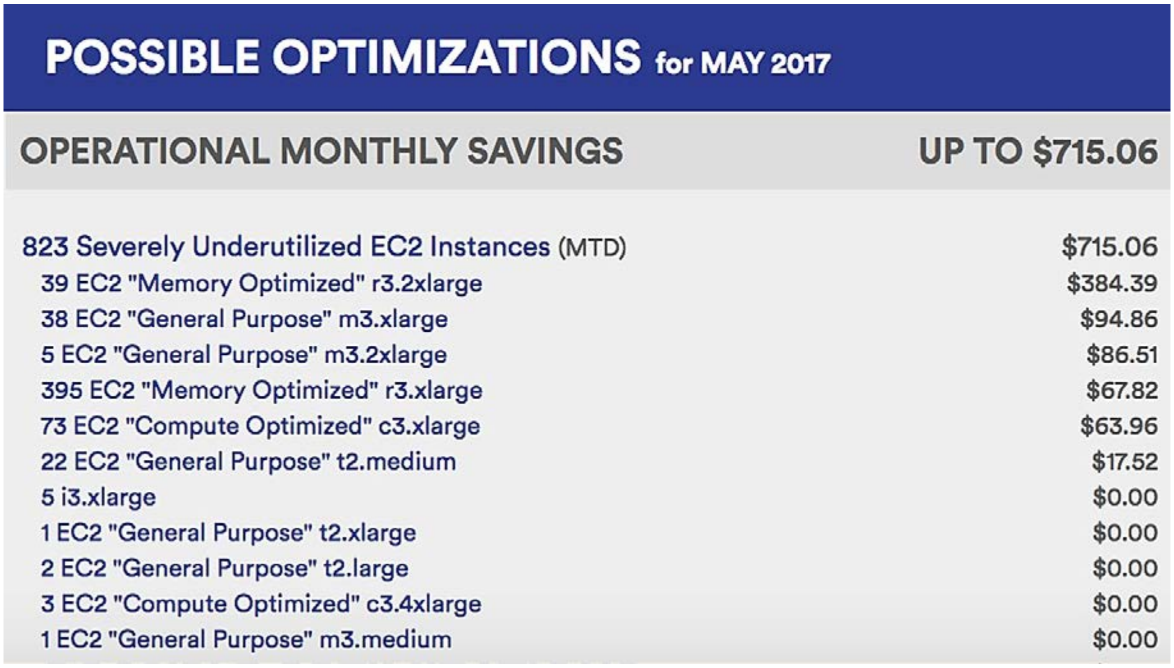
CloudHealth reports run for any timeframe – hourly, daily, weekly, monthly or annually – and you can save and subscribe to them for quick and easy access. To access the raw data, you can download metrics in a tabular format. In addition to tracking historical data, CloudHealth also forecasts for the future. Using past data, the platform can predict next month’s spend or tomorrow’s usage across hourly, daily, weekly or monthly intervals.



Performance Detail

Function: Cube Workers

INTERVAL: **HOURLY** | TOPIC: **MEMORY** | METRICS: (3) | TIME: **ALL AVAILABLE** | CHART: **LINE**



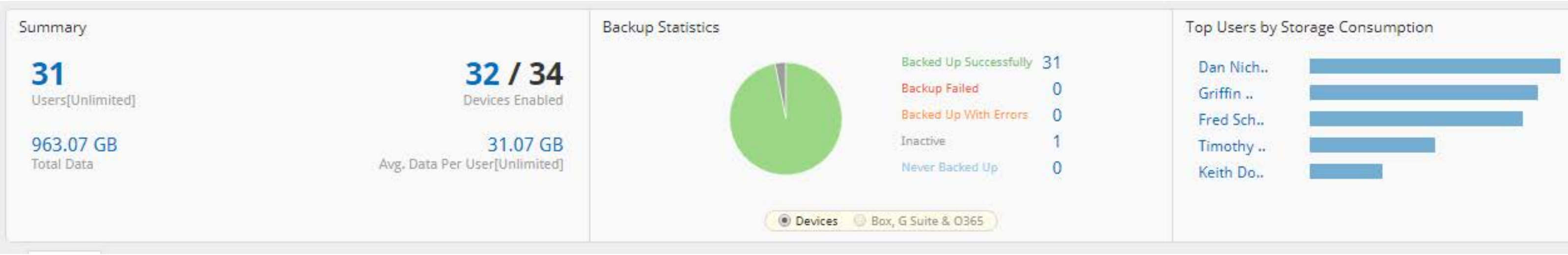
POSSIBLE OPTIMIZATIONS for MAY 2017

OPERATIONAL MONTHLY SAVINGS	UP TO $715.06
823 Severely Underutilized EC2 Instances (MTD)	$715.06
39 EC2 "Memory Optimized" r3.2xlarge	$384.39
38 EC2 "General Purpose" m3.xlarge	$94.86
5 EC2 "General Purpose" m3.2xlarge	$86.51
395 EC2 "Memory Optimized" r3.xlarge	$67.82
73 EC2 "Compute Optimized" c3.xlarge	$63.96
22 EC2 "General Purpose" t2.medium	$17.52
5 i3.xlarge	$0.00
1 EC2 "General Purpose" t2.xlarge	$0.00
2 EC2 "General Purpose" t2.large	$0.00
3 EC2 "Compute Optimized" c3.4xlarge	$0.00
1 EC2 "General Purpose" m3.medium	$0.00

Druva

Druva provides near real-time reporting on a variety of backup usage and performance statics which can be exported as reports and viewed over the web, by email, or locally downloaded. Druva allows you to create the following reports:

- Active Alerts
- Alert History
- Failed Backups
- Last Backup Status
- Restore Activity
- Sharing Usage
- Storage Status
- User Rollout
- Non-Compliance Report
- Preserved Users Report
- Salesforce Backup and Restore Report
- Unusual Data Activity Report
- Inactive Devices Report
- SharePoint Backup and Restore Report
- Complete Report



Summary

31
Users[Unlimited]

32 / 34
Devices Enabled

963.07 GB
Total Data

31.07 GB
Avg. Data Per User[Unlimited]

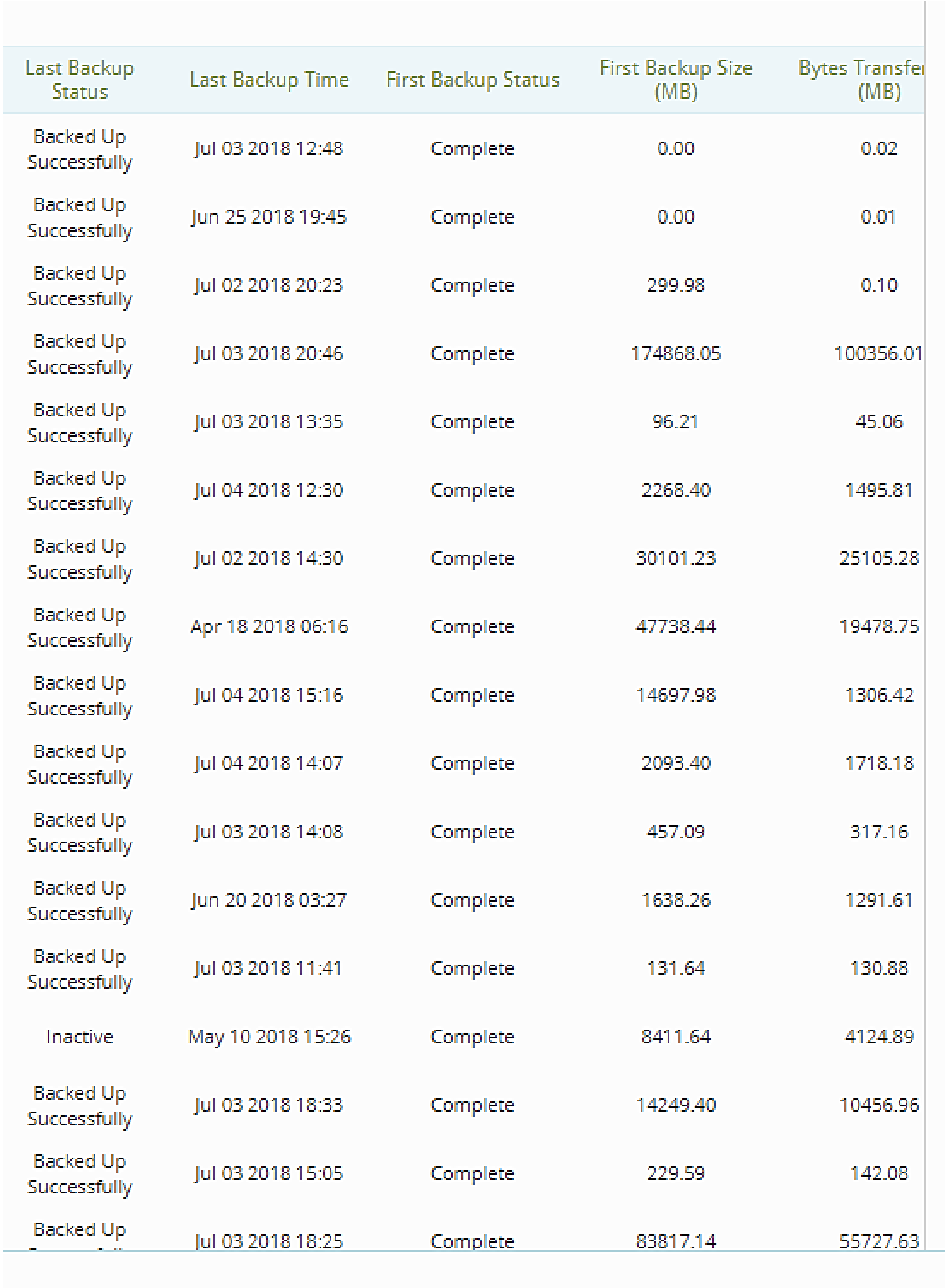
Backup Statistics

Backed Up Successfully	31
Backup Failed	0
Backed Up With Errors	0
Inactive	1
Never Backed Up	0

● Devices ○ Box, G Suite & O365

Top Users by Storage Consumption

Dan Nich..
Griffin ..
Fred Sch..
Timothy ..
Keith Do..

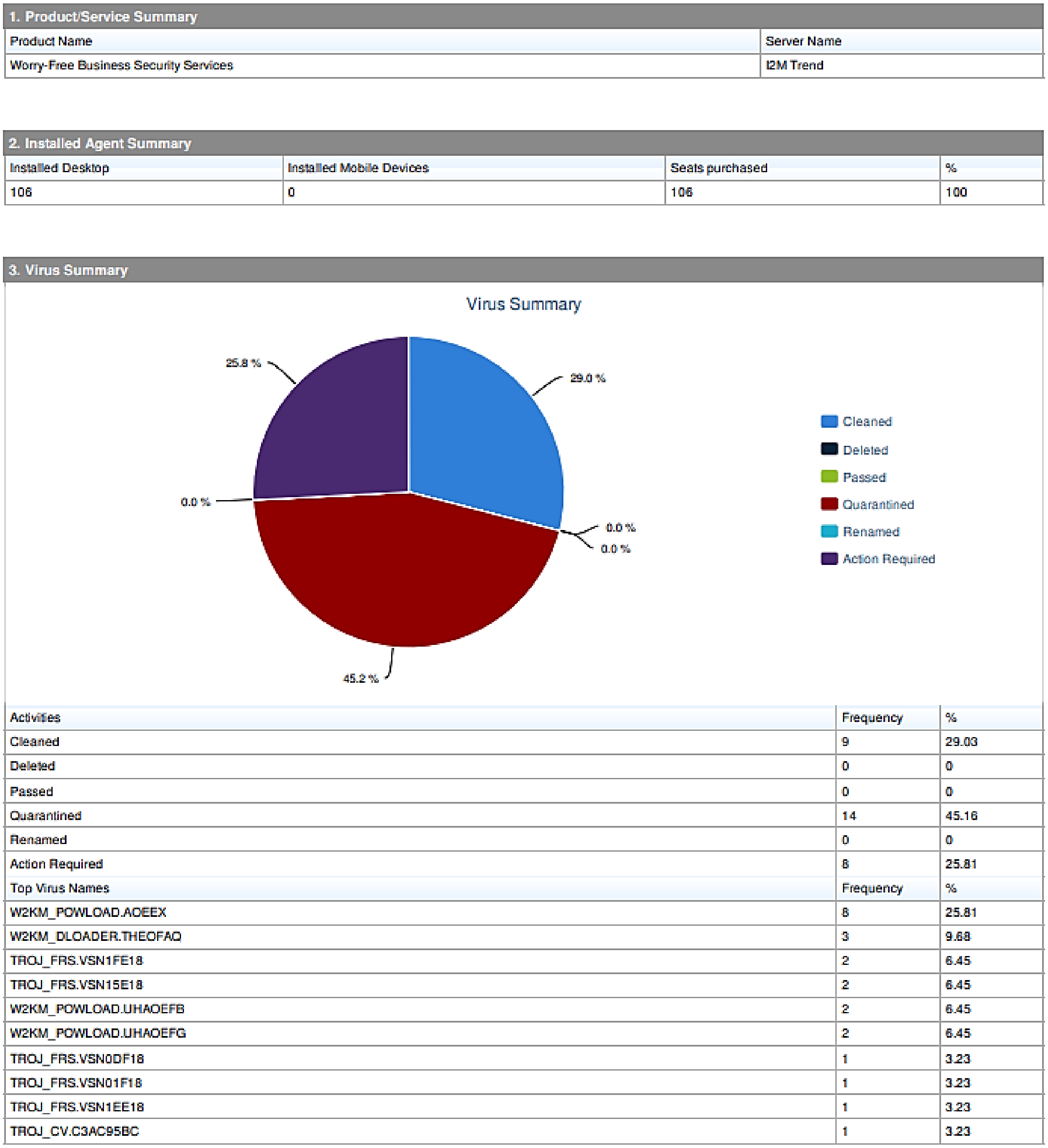


Last Backup Status	Last Backup Time	First Backup Status	First Backup Size (MB)	Bytes Transfer (MB)
Backed Up Successfully	Jul 03 2018 12:48	Complete	0.00	0.02
Backed Up Successfully	Jun 25 2018 19:45	Complete	0.00	0.01
Backed Up Successfully	Jul 02 2018 20:23	Complete	299.98	0.10
Backed Up Successfully	Jul 03 2018 20:46	Complete	174868.05	100356.01
Backed Up Successfully	Jul 03 2018 13:35	Complete	96.21	45.06
Backed Up Successfully	Jul 04 2018 12:30	Complete	2268.40	1495.81
Backed Up Successfully	Jul 02 2018 14:30	Complete	30101.23	25105.28
Backed Up Successfully	Apr 18 2018 06:16	Complete	47738.44	19478.75
Backed Up Successfully	Jul 04 2018 15:16	Complete	14697.98	1306.42
Backed Up Successfully	Jul 04 2018 14:07	Complete	2093.40	1718.18
Backed Up Successfully	Jul 03 2018 14:08	Complete	457.09	317.16
Backed Up Successfully	Jun 20 2018 03:27	Complete	1638.26	1291.61
Backed Up Successfully	Jul 03 2018 11:41	Complete	131.64	130.88
Inactive	May 10 2018 15:26	Complete	8411.64	4124.89
Backed Up Successfully	Jul 03 2018 18:33	Complete	14249.40	10456.96
Backed Up Successfully	Jul 03 2018 15:05	Complete	229.59	142.08
Backed Up	Jul 03 2018 18:25	Complete	83817.14	55727.63

Trend Micro
Worry Free Business Security Service
Trend Micro provides near real-time reporting on a variety of detailed performance and usage statics which can be exported as reports and viewed over the web, by email, or locally downloaded. Trend allows you to create reports for the following:

- Anti-Virus
- Anti-Spyware

- Web Reputation
- URL Filtering
- Behavior Monitoring
- Device Control
- Network Virus



1. Product/Service Summary	
Product Name	Server Name
Worry-Free Business Security Services	I2M Trend

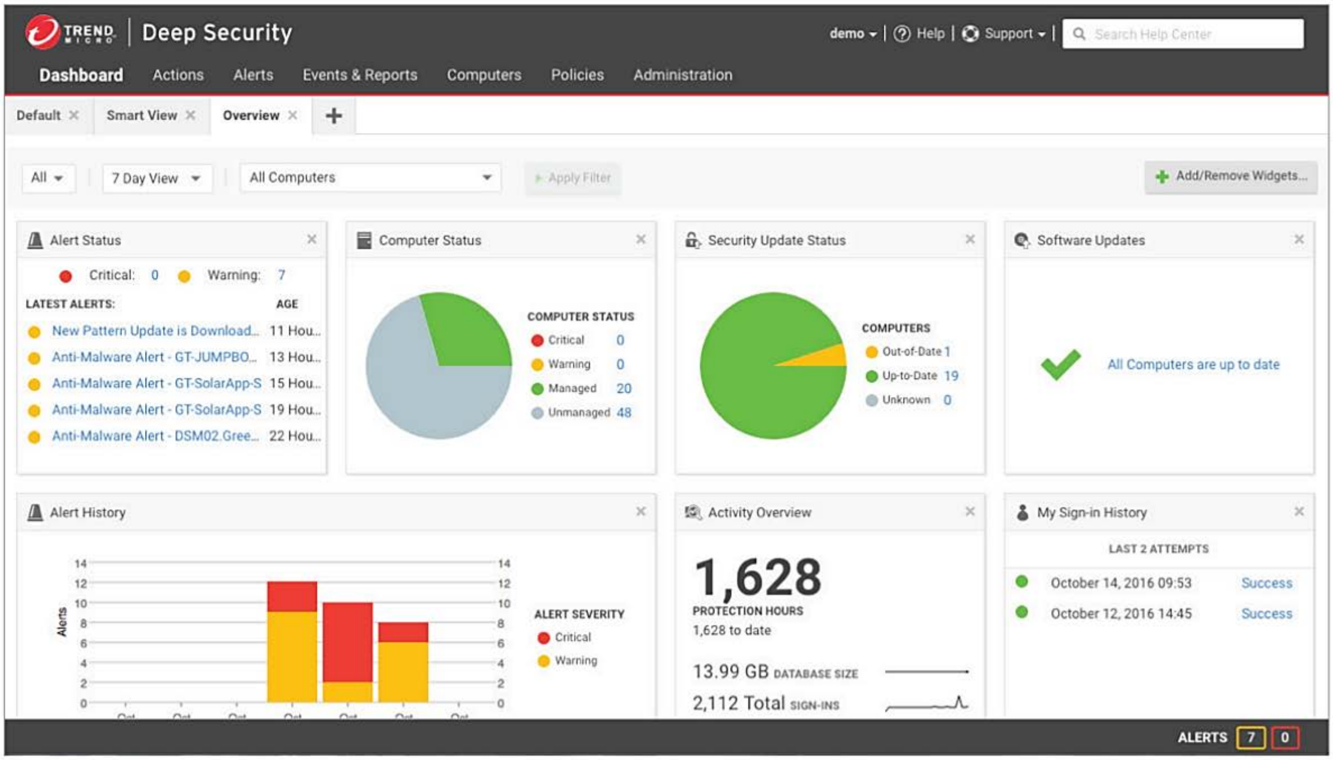
2. Installed Agent Summary			
Installed Desktop	Installed Mobile Devices	Seats purchased	%
106	0	106	100

3. Virus Summary

Activities	Frequency	%
Cleaned	9	29.03
Deleted	0	0
Passed	0	0
Quarantined	14	45.16
Renamed	0	0
Action Required	8	25.81
Top Virus Names	Frequency	%
W2KM_POWLOAD.AOEEX	8	25.81
W2KM_DLOADER.THEOFAQ	3	9.68
TROJ_FRS.VSN1FE18	2	6.45
TROJ_FRS.VSN15E18	2	6.45
W2KM_POWLOAD.UHAOEFB	2	6.45
W2KM_POWLOAD.UHAOEFG	2	6.45
TROJ_FRS.VSN0DF18	1	3.23
TROJ_FRS.VSN01F18	1	3.23
TROJ_FRS.VSN1EE18	1	3.23
TROJ_CV.C3AC95BC	1	3.23

Trend Micro
Deep Security As A Service (DSaaS)

Deep Security as a Service helps you resolve key business issues Virtual patching Shield vulnerabilities before they can be exploited and eliminate the operational pains of emergency patching, frequent patch cycles, and costly system downtime Zero-day security Protection against zero-day vulnerabilities while minimizing operational impact from resource inefficiencies and emergency patching Compliance Achieve and prove compliance with a number of regulatory requirements for PCI DSS, HIPAA, SANS, NIST, SSAE 16, and more Integrated security Shift from multiple point products to one trusted, complete security service.



Alert Status

● Critical: 0 ● Warning: 7

LATEST ALERTS:	AGE
● New Pattern Update is Download...	11 Hou...
● Anti-Malware Alert - GT-JUMPBO...	13 Hou...
● Anti-Malware Alert - GT-SolarApp-S	15 Hou...
● Anti-Malware Alert - GT-SolarApp-S	19 Hou...
● Anti-Malware Alert - DSM02.Gree...	22 Hou...

Computer Status

COMPUTER STATUS

● Critical	0
● Warning	0
● Managed	20
● Unmanaged	48

Security Update Status

COMPUTERS

● Out-of-Date	1
● Up-to-Date	19
● Unknown	0

Software Updates

✓ All Computers are up to date

Alert History

ALERT SEVERITY

● Critical

● Warning

Activity Overview

1,628

PROTECTION HOURS

1,628 to date

13.99 GB DATABASE SIZE

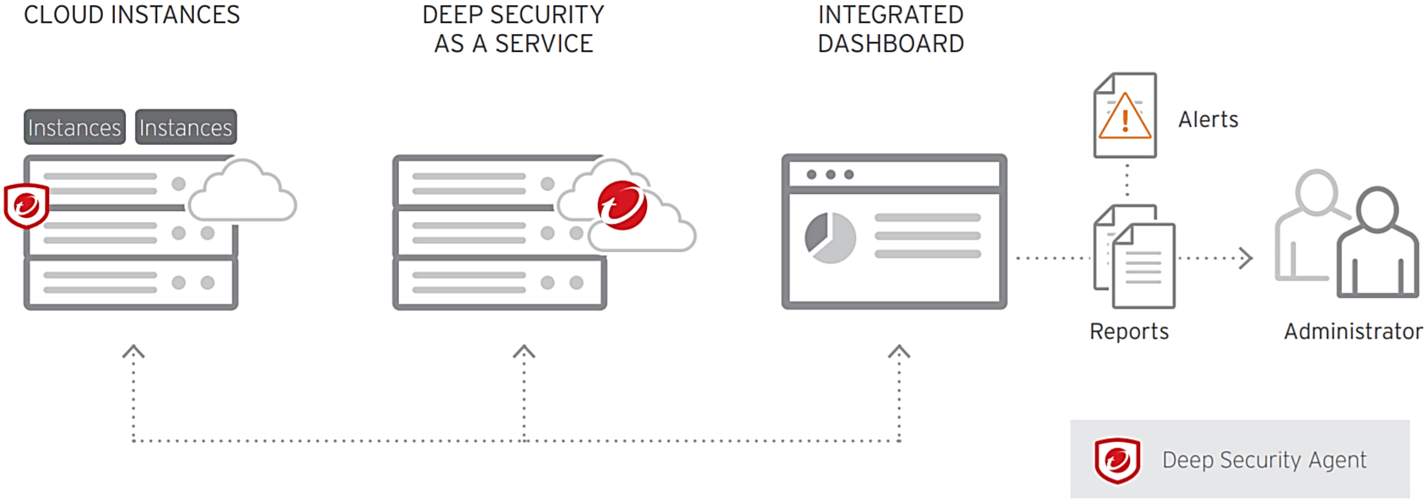
2,112 Total SIGN-INS

My Sign-in History

LAST 2 ATTEMPTS

●	October 14, 2016 09:53	Success
●	October 12, 2016 14:45	Success

ALERTS 7 0



SIMPLIFY SECURITY MANAGEMENT
• Reduces resources needed for set up and management
• Simplifies purchasing and management with multiple security controls in one product
• Lowers management costs by automating repetitive and resource intensive security tasks

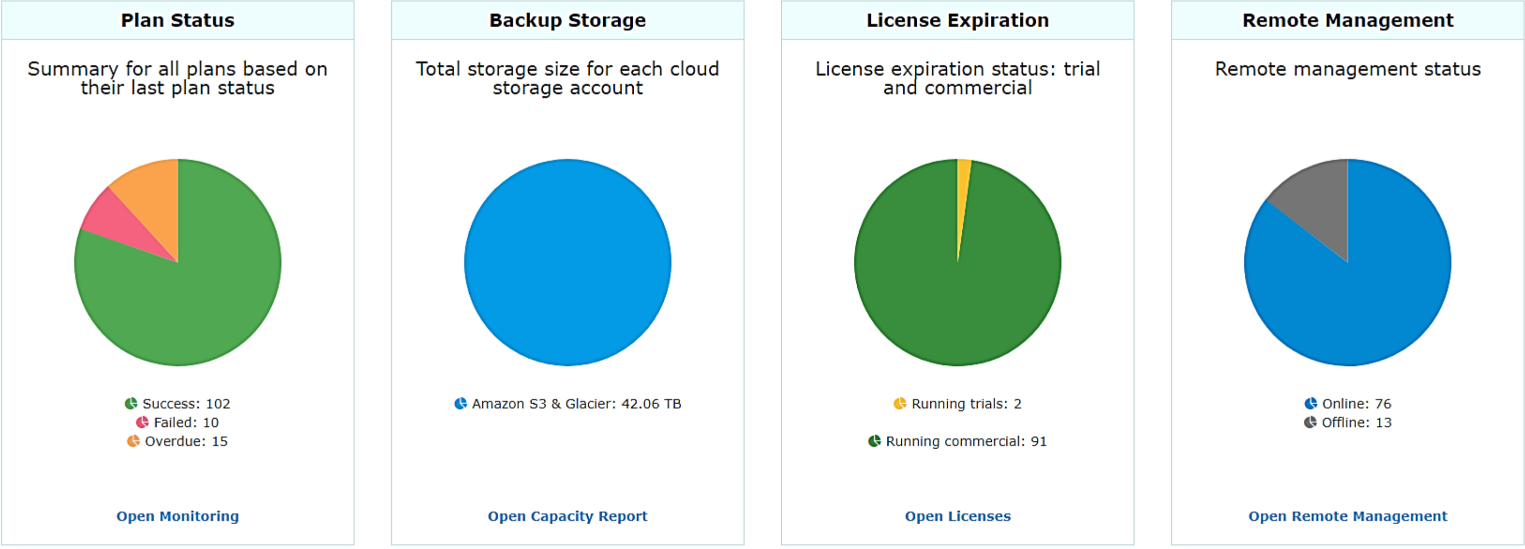
PREVENT DATA BREACHES AND BUSINESS DISRUPTIONS
• Immediately protects against vulnerabilities like Shellshock, Heartbleed , or WannaCry
• Blocks malware, including ransomware, that attempts to evade detection
• Locks down servers so that no unauthorized applications can run
• Ensures cloud servers only communicate with expected systems and safe domains
• Detects and alerts you of suspicious or malicious activity

ACHIEVE COST-EFFECTIVE COMPLIANCE
• Addresses major compliance requirements for PCI DSS, as well as HIPAA, NIST, SANS, and SSAE 16 with one solution
• Provides detailed, auditable reports that document prevented attacks and policy compliance status • Reduces the preparation time and effort required to support audits

CloudBerry
CloudBerry provides near real-time reporting on a variety of detailed performance and usage statics which can be exported as reports and viewed over the web, by email, or locally downloaded. Cloudberry allows you to create reports for the following:

- Storage Usage Report
    - Storage usage report contains information on the storage limits and space used for each user's storage destination.
- Group Report
    - Group Report contains information about the last backup plan run for each computer.
- Licensing Report
    - Licensing report contains information on existing trial and paid licenses, their activations and expirations for each user for the designated period.
- Overdue Report
    - Overdue Report displays information regarding the overdue backup plans execution for each user/company.
- License Usage Report

- A new licensing report that contains licenses usage info grouped by license type.



Plan Status

Summary for all plans based on their last plan status

Open Monitoring

Backup Storage

Total storage size for each cloud storage account

Open Capacity Report

License Expiration

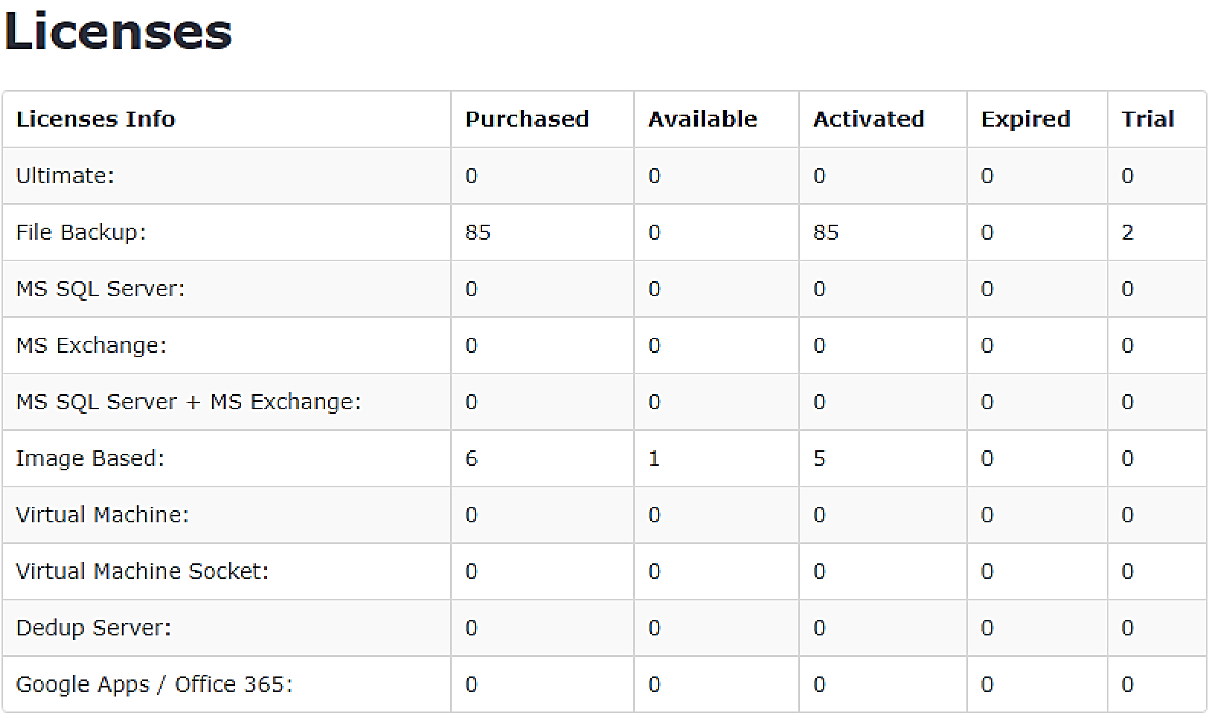
License expiration status: trial and commercial

Open Licenses

Remote Management

Remote management status

Open Remote Management



Licenses

Licenses Info	Purchased	Available	Activated	Expired	Trial
Ultimate:	0	0	0	0	0
File Backup:	85	0	85	0	2
MS SQL Server:	0	0	0	0	0
MS Exchange:	0	0	0	0	0
MS SQL Server + MS Exchange:	0	0	0	0	0
Image Based:	6	1	5	0	0
Virtual Machine:	0	0	0	0	0
Virtual Machine Socket:	0	0	0	0	0
Dedup Server:	0	0	0	0	0
Google Apps / Office 365:	0	0	0	0	0

DUO:
As new vulnerabilities are discovered, there are always more software updates, making it increasingly difficult for IT teams to understand their organization's overall security posture.

With Endpoint Visibility, Duo analyzes what’s running on all of your users’ devices, including all unmanaged PCs, Macs and mobile devices. Using this data, Duo provides an actionable security health report for IT admins, showing:

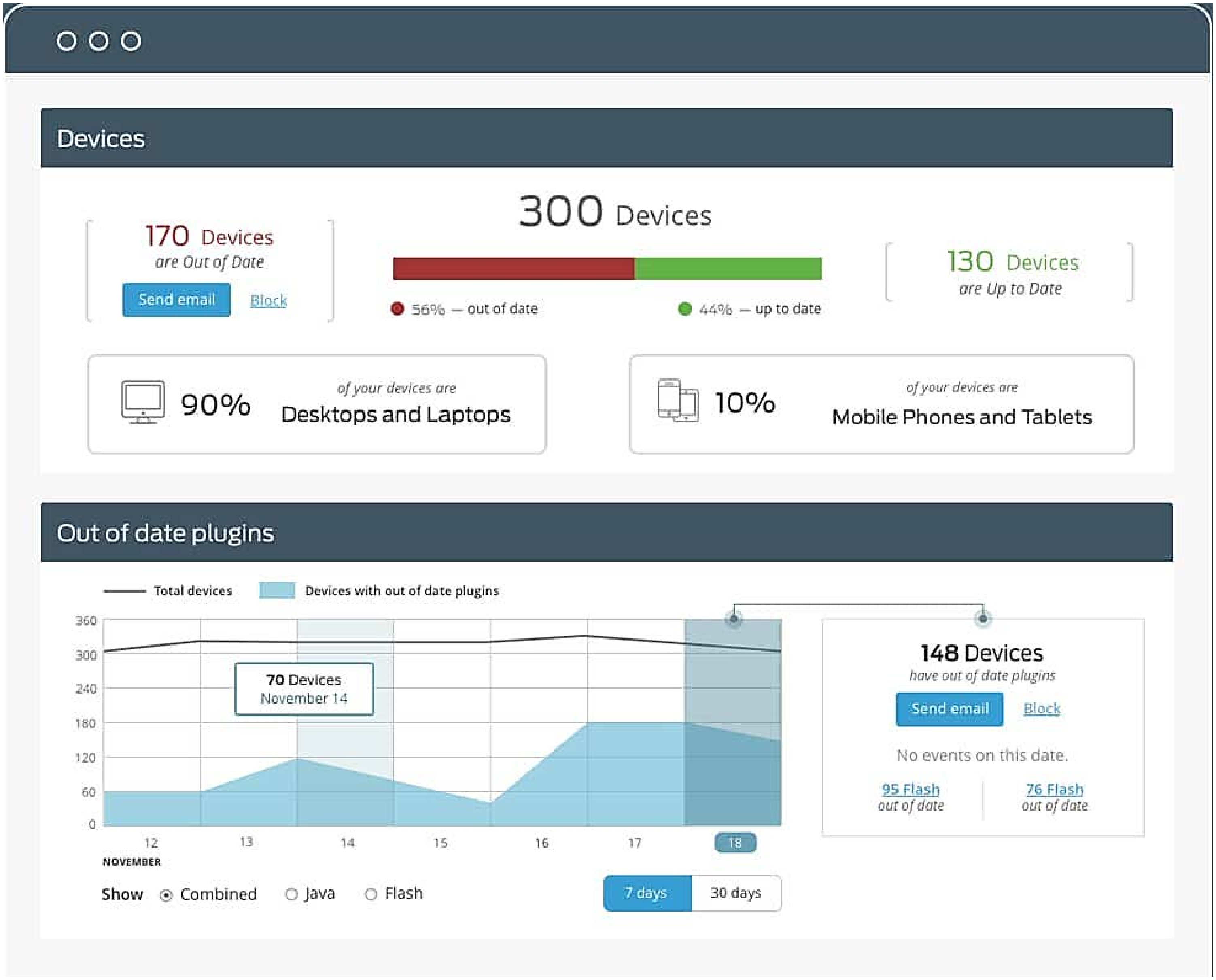
- An analysis of your users’ devices, including current device OS, browsers, Flash and Java versions
- Security health trends of all devices accessing your business applications, including which devices are outdated or updated by end users
- The latest security events that may result in outdated devices, including a new browser or plugin update released by a software vendor

All without the use of an agent, and exportable into PDF.

With these reports, admins can take action and notify users to update devices with Self-Remediation, or block outdated devices with Endpoint Remediation.

Deployment Progress Report
Run reports on the Success and Deployment metrics of your Duo environment. The Deployment Progress report gives you information on the state of your Duo enrollment across your organization.

Successful Authentication Report
The Successful Authentication report provides information about the success rate of authentications, authentication activity over a period of time, authentication methods and top applications.



Devices

300 Devices

170 Devices are Out of Date

● 56% — out of date

● 44% — up to date

130 Devices are Up to Date

90% of your devices are Desktops and Laptops

10% of your devices are Mobile Phones and Tablets

Out of date plugins

70 Devices November 14

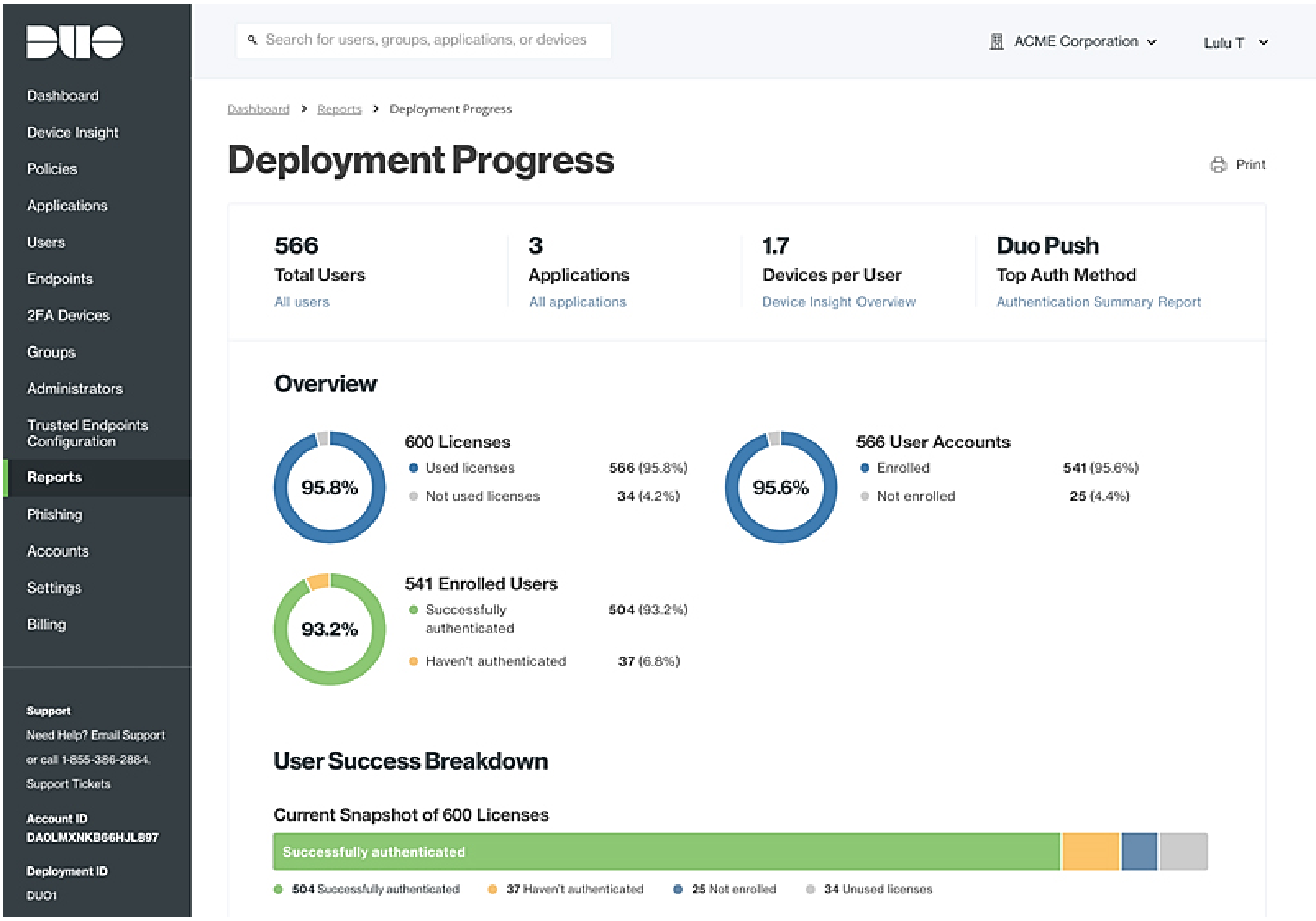
148 Devices have out of date plugins

No events on this date.

95 Flash out of date

76 Flash out of date

Show ◉ Combined ○ Java ○ Flash



Support
Need Help? Email Support or call 1-855-386-2884.
Support Tickets

Account ID
DA0LMXNKB66HJL897

Deployment ID
DUO1

Deployment Progress

566 Total Users
All users

3 Applications
All applications

1.7 Devices per User
Device Insight Overview

Duo Push Top Auth Method
Authentication Summary Report

Overview

95.8%

600 Licenses

● Used licenses	566 (95.8%)
● Not used licenses	34 (4.2%)

95.6%

566 User Accounts

● Enrolled	541 (95.6%)
● Not enrolled	25 (4.4%)

93.2%

541 Enrolled Users

● Successfully authenticated	504 (93.2%)
● Haven't authenticated	37 (6.8%)

User Success Breakdown

Current Snapshot of 600 Licenses

Successfully authenticated

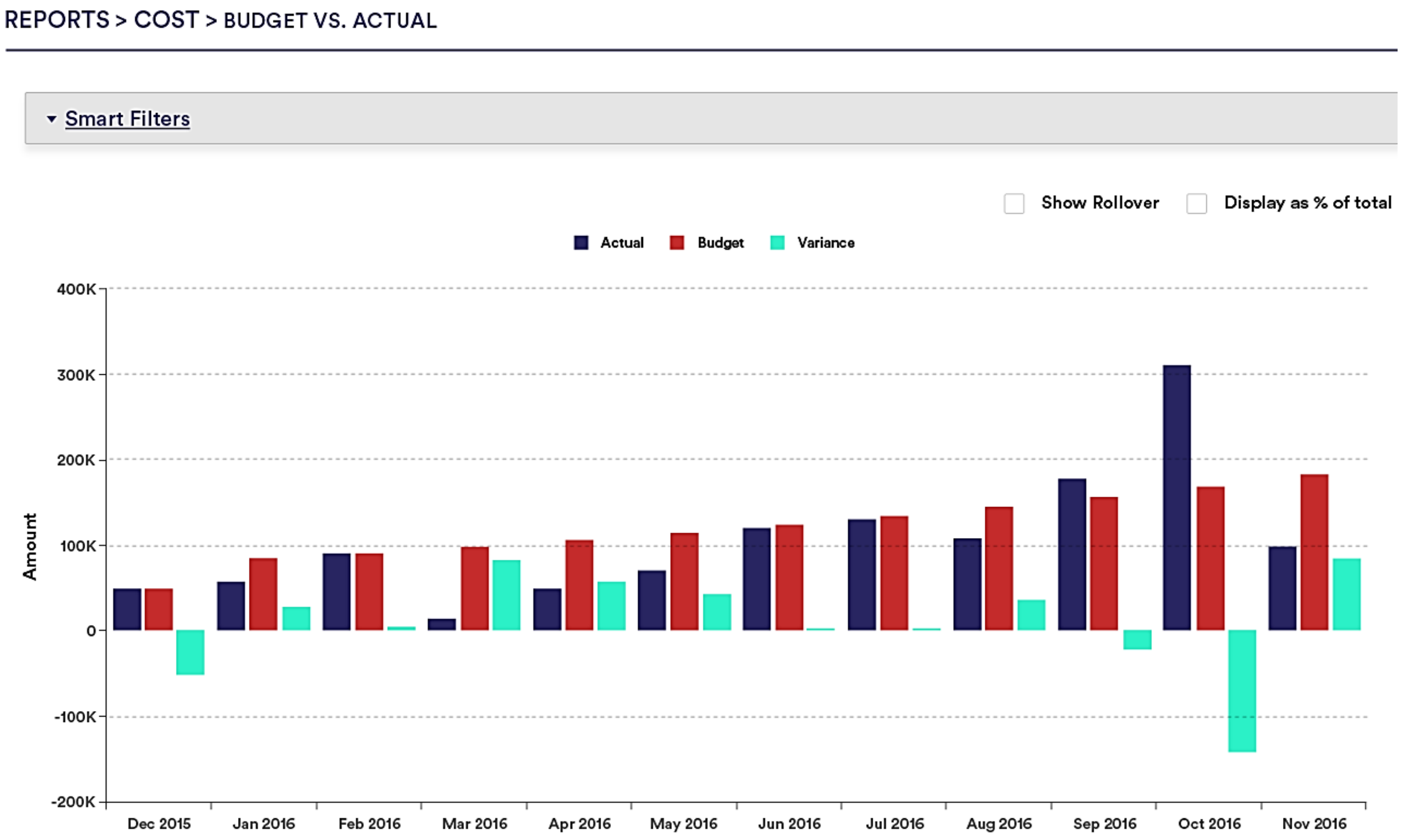
● 504 Successfully authenticated ● 37 Haven't authenticated ● 25 Not enrolled ● 34 Unused licenses

8.12.8

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

Response:

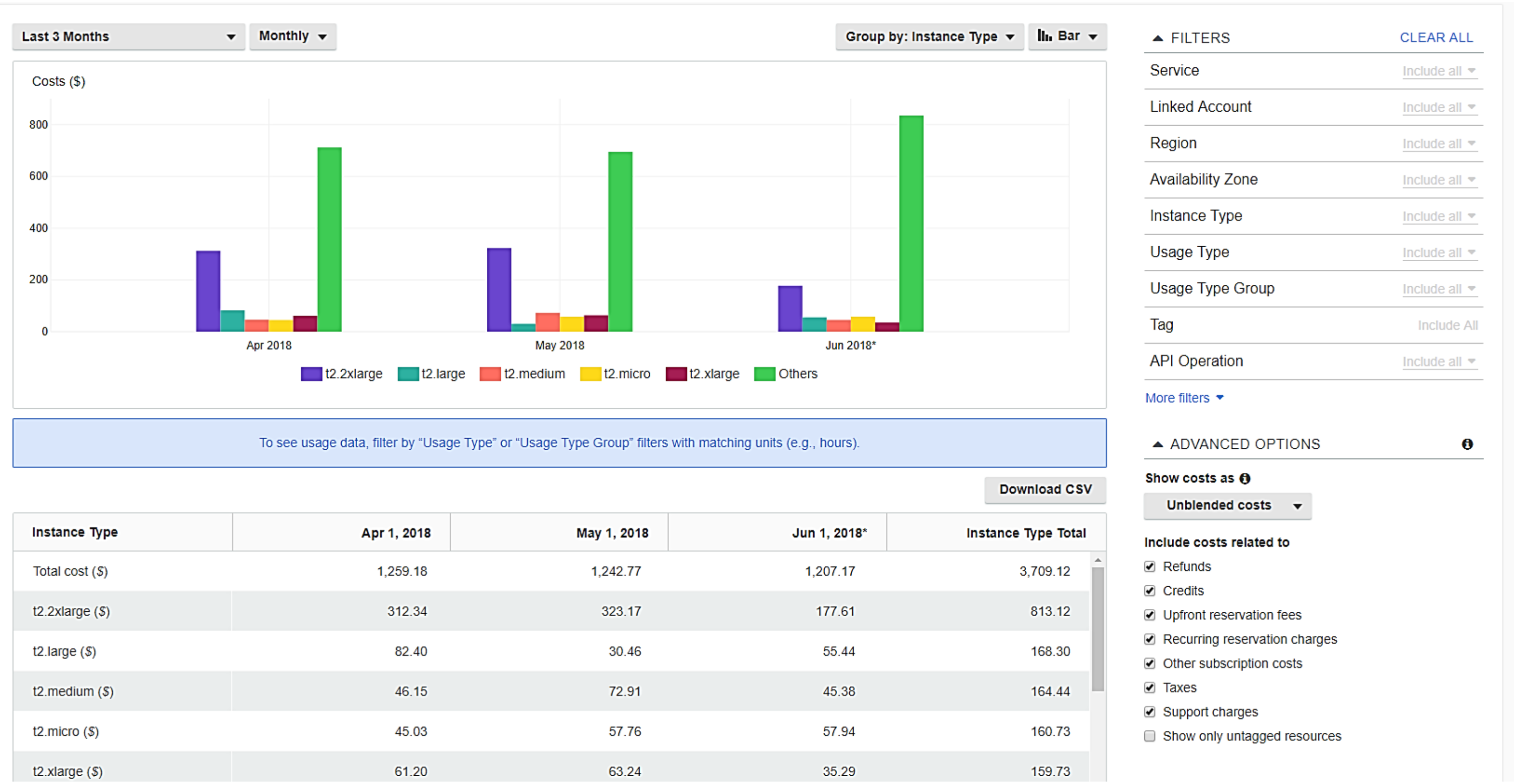
i2m provides the purchasing entity the capability to print historical, statistical, and usage reports locally. Electronic copies of reports can be delivered by email are downloaded over the web for local viewing. Historical, statistical, and usage reports can be scheduled to send via email at monthly, weekly, daily, hourly, etc. schedule or downloaded on-demand. Standard reports and well as customized reports are configured to illustrate adherence to contracted SLAs and compliance requirements. Additional reports can be configured and tailored to the needs of the Purchasing Entity on request.



REPORTS > COST > BUDGET VS. ACTUAL

▾ Smart Filters

□ Show Rollover □ Display as % of total



To see usage data, filter by "Usage Type" or "Usage Type Group" filters with matching units (e.g., hours).

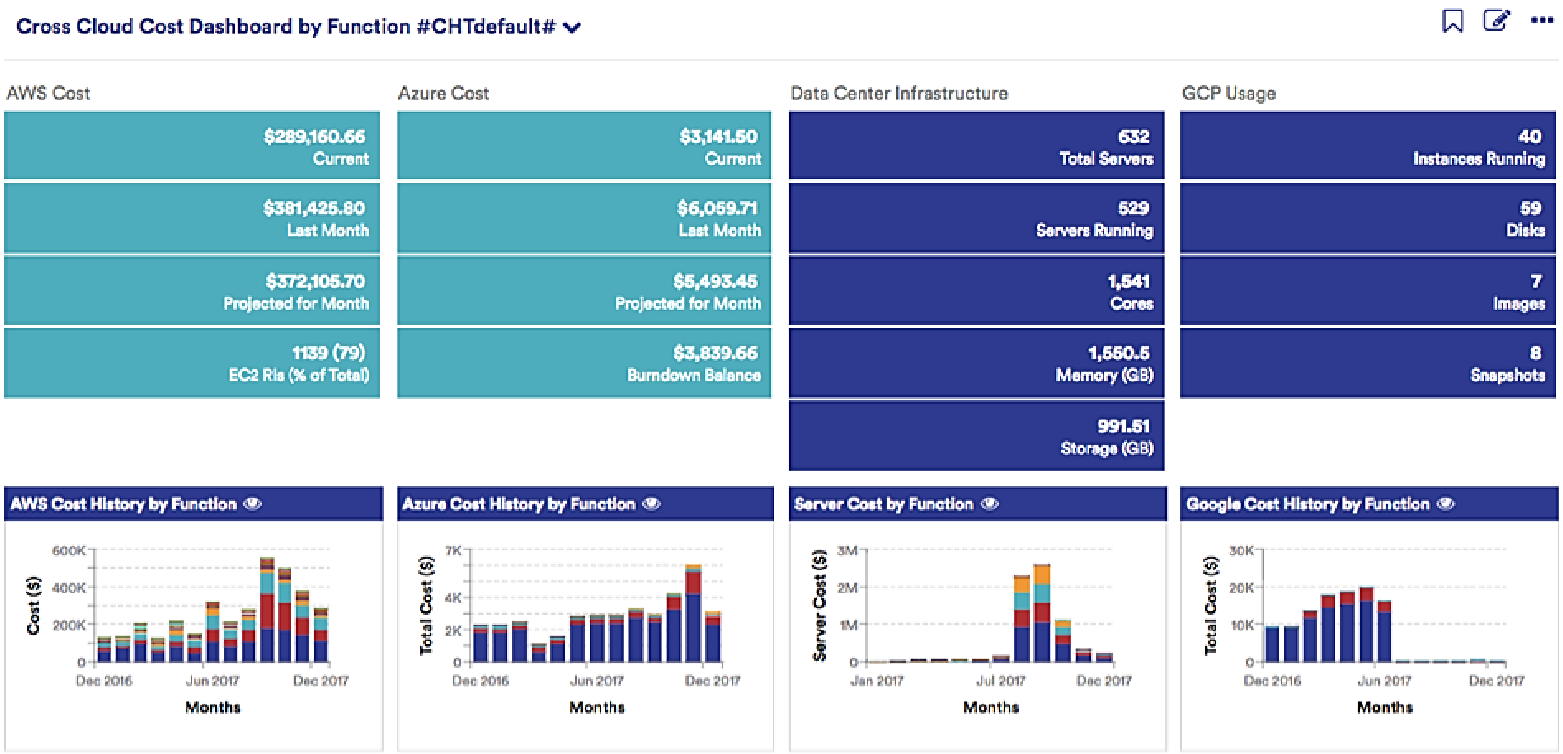
Instance Type	Apr 1, 2018	May 1, 2018	Jun 1, 2018*	Instance Type Total
Total cost ($)	1,259.18	1,242.77	1,207.17	3,709.12
t2.2xlarge ($)	312.34	323.17	177.61	813.12
t2.large ($)	82.40	30.46	55.44	168.30
t2.medium ($)	46.15	72.91	45.38	164.44
t2.micro ($)	45.03	57.76	57.94	160.73
t2.xlarge ($)	61.20	63.24	35.29	159.73

Service	Include all
Linked Account	Include all
Region	Include all
Availability Zone	Include all
Instance Type	Include all
Usage Type	Include all
Usage Type Group	Include all
Tag	Include All
API Operation	Include all

Show costs as: Unblended costs

Include costs related to

- ☑ Refunds
- ☑ Credits
- ☑ Upfront reservation fees
- ☑ Recurring reservation charges
- ☑ Other subscription costs
- ☑ Taxes
- ☑ Support charges
- ☐ Show only untagged resources



AWS Cost	Azure Cost	Data Center Infrastructure	GCP Usage
$289,160.66 Current	$3,141.50 Current	632 Total Servers	40 Instances Running
$381,425.80 Last Month	$6,059.71 Last Month	529 Servers Running	59 Disks
$372,105.70 Projected for Month	$5,493.45 Projected for Month	1,541 Cores	7 Images
1139 (79) EC2 RIs (% of Total)	$3,839.66 Burndown Balance	1,550.5 Memory (GB)	8 Snapshots
		991.51 Storage (GB)	

8.12.9

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

Response:

Amazon Web Services

The Purchasing Entities can utilize the AWS Management Console, AWS Command Line Interface, or other deployment methods for on-demand deployment of all AWS Services at any time (24x365).

Druva

The Purchasing Entity can utilize the Druva Management Console for on-demand deployment of user accounts for Druva inSync Endpoint Backup and other Druva related services. The console can be accessed over the web.

Trend Micro

The Purchasing Entity can utilize the Trend Micro Remote Manager Console for on-demand deployment of the Trend Micro Worry-Free Endpoint protection agent for devices. The console can be accessed over the web

CloudBerry

The Purchasing Entity can utilize the CloudBerry Management Console for on-demand provisioning of CloudBerry device licenses' in order to deploy the Cloudberry Backup agent on devices. The console can be accessed over the web.

CloudHealth

The Purchasing Entity can provision on-demand cloud costs, usage, security, and performance reports from the CloudHealth console. The console can be accessed over the web.

DUO

Duo provides an admin portal which controls all additions deletions and management of user accounts which can be executed on-demand with no limitation on quantity.

8.12.10

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

Response:

Amazon Web Service

- **Amazon Auto Scaling**
  AWS Auto Scaling monitors your applications and automatically adjusts capacity to

maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas. AWS Auto Scaling makes scaling simple with recommendations that allow you to optimize performance, costs, or balance between them.

AWS Auto Scaling lets you set target utilization levels for multiple resources in a single, intuitive interface. You can quickly see the average utilization of all of your scalable resources without having to navigate to other consoles. For example, if your application uses Amazon EC2 and Amazon DynamoDB, you can use AWS Auto Scaling to manage resource provisioning for all of the EC2 Auto Scaling groups and database tables in your application.

AWS Auto Scaling lets you build scaling plans that automate how groups of different resources respond to changes in demand. You can optimize availability, costs, or a balance of both. AWS Auto Scaling automatically creates all of the scaling policies and sets targets for you based on your preference. AWS Auto Scaling monitors your application and automatically adds or removes capacity from your resource groups in real-time as demands change.

Using AWS Auto Scaling, you maintain optimal application performance and availability, even when workloads are periodic, unpredictable, or continuously changing. AWS Auto Scaling continually monitors your applications to make sure that they are operating at your desired performance levels. When demand spikes, AWS Auto Scaling automatically increases the capacity of constrained resources so you maintain a high quality of service.

- **Amazon Elastic Load Balancer**
  Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault tolerant.

  Elastic Load Balancing is capable of handling rapid changes in network traffic patterns. Additionally, deep integration with Auto Scaling ensures sufficient application capacity to meet varying levels of application load without requiring manual intervention.

Elastic Load Balancing automatically distributes incoming traffic across multiple targets – Amazon EC2 instances, containers, and IP addresses – in multiple Availability Zones and ensures only healthy targets receive traffic. Elastic Load Balancing can also load balance across a Region, routing traffic to healthy targets in different Availability Zones.

- **Amazon EC2**
  Amazon EC2 Auto Scaling helps you maintain application availability and allows you to dynamically scale your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Amazon EC2 Auto Scaling for fleet management of EC2 instances to help maintain the health and availability of your fleet and ensure that you are running your desired number of Amazon EC2 instances. You can also use Amazon EC2 Auto Scaling for dynamic scaling of EC2 instances in order to automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs. Amazon EC2 Auto Scaling is well suited both to applications that have stable demand patterns or that experience hourly, daily, or weekly variability in usage.

  Improve Fault Tolerance with Amazon EC2 Auto Scaling which can detect when an instance is unhealthy, terminate it, and replace it with a new one. Increase application availability with Amazon EC2 Auto Scaling which ensures that your application always has the right amount of compute capacity.

- **Amazon CloudWatch**
  Auto Scaling sends metrics for instances and groups to CloudWatch. For Auto Scaling instances, you can enable detailed (one-minute) monitoring or basic (five-minute) monitoring. The following metrics are used by AWS Auto Scaling in order to manage your scale-up/scale-down policies:

  - GroupMinSize
    - The minimum size of the Auto Scaling group.
  - GroupMaxSize
    - The maximum size of the Auto Scaling group.
  - GroupDesiredCapacity
    - The number of instances that the Auto Scaling group attempts to maintain.
  - GroupInServiceInstances
    - The number of instances that are running as part of the Auto Scaling group. This metric does not include instances that are pending or

terminating.

- GroupPendingInstances
    - The number of instances that are pending. A pending instance is not yet in service. This metric does not include instances that are in service or terminating.

- GroupStandbyInstances
    - The number of instances that are in a Standby state. Instances in this state are still running but are not actively in service.

- GroupTerminatingInstances
    - The number of instances that are in the process of terminating. This metric does not include instances that are in service or pending.

- GroupTotalInstances
    - The total number of instances in the Auto Scaling group. This metric identifies the number of instances that are in service, pending, and terminating.

CloudHealth

- **On-demand self-service**
  CloudHealth integrates with AWS, GCP, Azure and Local Data centers or Colocation to provide on-demand cost, usage, billing reports, and automated governance actions to enable resource management and optimization without human intervention or alert and resolve for services that fall out of compliance. Where admins can integrate into these CSPs and their Local Infrastructure on the fly and data collection, alerting and remediation begin immediately.
- **Rapid elasticity**
  Data that CloudHealth collects from the consumers Amazon Web Services account can be expanded to indulge all available data or confined to collect only certain data which is applicable or requested by the consumer. There is no limit on the amount of accounts, users, reports or governance actions you are allowed to generate through CloudHealth. The Service simple scales up and down with consumer demand

CloudBerry

- **On-demand self-service**
  Cloudberry provides a central web management console that can be used to provision on-demand storage and licenses to run different the versions of the CloudBerry backup agents.
- **Rapid elasticity**

Capacity for the cloudberry licenses and backup storage can be provisioned and released on demand or automatically based on usage activity or consumer demand. Capabilities for provisioning storage and licenses appear unlimited and can be appropriated in any quantity at any time.

Druva

- **On-demand self-service**
  Druva backup agent's licenses and storage can be provisioned on-demand through a central Druva web management console without requiring human interaction with the service provider.
- **Rapid elasticity**
  Storage capacity and user licenses are monitored for resource usage and can be provisioned and released on-demand or automatically based on usage activity. Capabilities for provisioning storage and licenses appear unlimited and can be appropriated in any quantity at any time.

DUO

- **On-demand self-service**
  Duo provides an admin portal which controls all additions deletions and management of user accounts which can be executed on-demand with no limitation on quantity.
- **Rapid elasticity**
  You rapidly scale the use of the SaaS service solutions on demand without any limitations to user accounts or devices managed. Users Accounts can be added removed elastically to scale usage and cost with the organization's needs.

Trend Micro

- **On-demand self-service**
  Trend Micro agent licenses can be provisioned on demand without requiring human interaction with the service provider.
- **Rapid elasticity**
  Trend Micro licenses can be provisioned and released on-demand to scale rapidly outward and inward based consumer demand or usage activity. Trend Micro licenses can be appropriated in any quantity at any time.

8.13 (E) CLOUD SECURITY ALLIANCE

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

Response:

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

- **Amazon Web Services**
  Amazon Web Services is a CSA Executive Member. Amazon web services has completed their own CSA Star Self-Assessment which we will be uploading along with this technical response.

  For more detailed information about Amazon Web Services and CSA, go to this webpage: https://aws.amazon.com/compliance/csa/

- **Trend Micro**
  Trend Micro is a CSA Corporate Member. A CAIQ will be uploaded along with this technical response.

- **CloudHealth**
  CloudHealth is a CSA Corporate Member. A CAIQ will be uploaded along with this technical response.

- **CloudBerry**
  CloudBerry is not a CSA Corporate Member. A CAIQ will be uploaded along with this technical response.

- **DUO**
  DUO is a CSA Corporate Member. A CAIQ will be uploaded along with this technical response.

- **Druva**
  Druva is a CSA Corporate Member. A CAIQ will be uploaded along with this technical response.

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

- **Amazon Web Services**
  Amazon web services has completed their own CSA Star Self-Assessment which we will be uploading along with this technical response. A CAIQ will be uploaded along with this technical response. This should satisfy the requirements for the completion of Exhibits 1 and 2.

  For more detailed information about Amazon Web Services and CSA, go to this webpage: https://aws.amazon.com/compliance/csa/

- **Trend Micro**
  A CAIQ will be uploaded along with this technical response which should satisfy the completion of Exhibit 1 only.

- **CloudHealth**
  A CAIQ will be uploaded along with this technical response which should satisfy the completion of Exhibit 1 only.

- **CloudBerry**
  A CAIQ will be uploaded along with this technical response which should satisfy the completion of Exhibit 1 only.

- **DUO**
  A CAIQ will be uploaded along with this technical response which should satisfy the completion of Exhibit 1 only.

- **Druva**
  A CAIQ will be uploaded along with this technical response which should satisfy the completion of Exhibit 1 only.

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

- **Amazon Web Services**
  AWS aligns with the CSA STAR Attestation and Certification based on the determinations in our third-party audits for System and Organization Controls (SOC) 2 Reports and ISO 27001. CSA STAR Level 2 Attestation is based on SOC 2. The SOC 2 Report attests that AWS has been validated by a third-party auditor to confirm that AWS control objectives are appropriately designed and are operating effectively. The CSA Star Attestations for Amazon Web Services will be uploaded along with this technical response.

- **Druva**
  There is currently no available certification to determine alignment.

- **Trend Micro**
  There is currently no available certification to determine alignment.

- **DUO**
  There is currently no available certification to determine alignment.

- **CloudBerry**

There is currently no available certification to determine alignment.

- **CloudHealth**
  There is currently no available certification to determine alignment.

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

- **Amazon Web Services**
  AWS provides customers with the tools they need to meet continuous monitoring requirements. CSA is still defining the Level 3 Continuous Monitoring requirements, so there is no available certification to determine alignment. However, customers can use the AWS Security by Design (SbD) program to provide control responsibilities outlines, the automation of security baselines, the configuration of security, and the customer audit of controls for AWS customer infrastructure, operating systems, services, and applications running in AWS. This standardized, automated, prescriptive, and repeatable design can be deployed for common use cases, security standards, and audit requirements across multiple industries and workloads. For more information, see the AWS Security by Design webpage.

- **Druva**
  There is currently no available certification to determine alignment.

- **Trend Micro**
  There is currently no available certification to determine alignment.

- **DUO**
  There is currently no available certification to determine alignment.

- **CloudBerry**
  There is currently no available certification to determine alignment.

- **CloudHealth**
  There is currently no available certification to determine alignment.

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.

Response:
Emergency or rush services process with NASPO ValuePoint Purchasing Entities:

Post project or service delivery implementations NASPO ValuePoint and its Purchasing Entities shall send any request for any products/services support, general questions and additional account creation requests to support@i2m.cloud. Please preface any requests that are an Emergency or Urgent as seen below.

Email should have subject line "NASPO ValuePoint – Support Request – The Members Legal Business Name – Emergency/Urgent – Short Description of Issue"

In the body of the request please include in detail the nature of your request, the products/services you need assistance with and primary point of contact if different from the requester.

At any time NASPO ValuePoint and its Purchasing Entities need to speak to an executive for any reason please contact them below:

Ahmed Attalla	President, i2m.cloud	ahmeda@i2m.cloud	267-240-9097
Hany Ahmed	Tech Services Manager	hanya@i2m.solutions	267-694-8053
Scott Miller	COO, i2m	scottm@i2m.solutions	484-238-4118
Steven Grzywinski	President and CTO, i2m	steveg@i2m.solutions	484-433-7136

8.14.2

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

Response:
Please see response for section 8.3.7 which details the response to this question.

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.

Amazon Web Services
Amazon Glacier allows the Purchasing Entity to easily designate the records retention time frame to retain regulatory archives in the original form for the required duration, and also place legal holds to retain data indefinitely until the hold is removed. A legal hold can be initiated on data by creating a vault access policy that denies the use of Glacier's Delete functions if the vault is tagged in a particular way. In addition to time-based retention and legal hold, Glacier Vault Lock can be used to implement a variety of compliance controls

which can be made immutable for strong governance, such as enforcing Multifactor Authentication on all data access/read activities to a vault with classified information.

You can deploy a variety of compliance controls with Vault Lock using the AWS Identity and Access Management (IAM) policy language. You can also test the full effect of these controls and fine-tune them before you lock the policy down. A locked policy cannot be deleted or altered once set, making Vault Lock ideal for customers in regulated industries that require tight controls on how business records must be retained before they can be erased.

Druva
Druva’s Endpoint backup features the ability to place a legal hold to preserve user backup data and avoid data deletion. When you put a user on legal hold, the user data from endpoints such as laptops and mobile, and from cloud applications is preserved.

CloudBerry
CloudBerry uses Amazon S3 for backup storage. The backup data is stored in the Participating Entities’ AWS account and can be transitioned from Amazon S3 to Amazon Glacier. Once the data is in Amazon Glacier, it can then utilize the legal hold functionality of Amazon Glacier’s Vault Lock service as mentioned above in this section.

CloudHealth
CloudHealth ingests data from the Participating Entities AWS account. That data is stored in Amazon S3. The data can be transitioned from Amazon S3 to Amazon Glacier in order to utilize the legal hold functionality of Amazon Glacier’s Vault Lock service as mentioned above in this section.

Trend
Trend Micro does not have the capability to place legal holds on data it collects.

DUO
Awaiting more information from DUO. Can be available on-demand when requested

8.15.2

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

Response:
Please see section 8.8 about Service or Data Recovery which responds to these DR risks and provides mitigation strategies. Below is how i2m aligns with the AWS Well Architected framework and the mitigation strategies taken.

The 5 Pillars of the AWS Well-Architected Framework

When architecting technology solutions on Amazon Web Services (AWS), if you neglect the five pillars of operational excellence, security, reliability, performance efficiency, and cost optimization, it can become challenging to build a system that delivers on your expectations and requirements. Incorporating these pillars into your architecture helps produce stable and efficient systems. This allows you to focus on the other aspects of design, such as functional requirements.

The AWS Well-Architected Framework helps cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and AWS Partner Network (APN) Partners to evaluate architectures, and provides guidance to implement designs that scale with your application needs over time.

1. Operational Excellence

The operational excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. You can find prescriptive guidance on implementation in the Operational Excellence Pillar whitepaper.

Design Principles
There are six design principles for operational excellence in the cloud:

- Perform operations as code
- Annotate documentation
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures
- Best Practices
- Operations teams need to understand their business and customer needs so they can support business outcomes. Ops creates and uses procedures to respond to operational events, and validates their effectiveness to support business needs. Ops also collects metrics that are used to measure the achievement of desired business outcomes.

Everything continues to change your business context, business priorities, customer needs, etc. It’s important to design operations to support evolution over time in response to change and to incorporate lessons learned through their performance.

2. Security

The security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies. You can find prescriptive guidance on implementation in the Security Pillar whitepaper.

Design Principles

There are six design principles for security in the cloud:

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Prepare for security events
- Best Practices
- Before you architect any system, you need to put in place practices that influence security. You will want to control who can do what. In addition, you want to be able to identify security incidents, protect your systems and services, and maintain the confidentiality and integrity of data through data protection.

You should have a well-defined and practiced process for responding to security incidents. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations. The AWS Shared Responsibility Model enables organizations to achieve security and compliance goals. Because AWS physically secures the infrastructure that supports our cloud services, you can focus on using services to accomplish your goals.

3. Reliability

The reliability pillar includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. You can find prescriptive guidance on implementation in the Reliability Pillar whitepaper.

Design Principles

There are five design principles for reliability in the cloud:

- Test recovery procedures
- Automatically recover from failure
- Scale horizontally to increase aggregate system availability
- Stop guessing capacity

- Manage change in automation
- Best Practices
- To achieve reliability, a system must have a well-planned foundation and monitoring in place, with mechanisms for handling changes in demand or requirements. The system should be designed to detect failure and automatically heal itself.

Before architecting any system, foundational requirements that influence reliability should be in place. For example, you must have sufficient network bandwidth to your data center. These requirements are sometimes neglected (because they are beyond a single project’s scope). This neglect can have a significant impact on the ability to deliver a reliable system. In an on-premises environment, these requirements can cause long lead times due to dependencies and therefore must be incorporated during initial planning.

With AWS, most of these foundational requirements are already incorporated or may be addressed as needed. The cloud is designed to be essentially limitless, so it is the responsibility of AWS to satisfy the requirement for sufficient networking and compute capacity, while you are free to change resource size and allocation, such as the size of storage devices, on demand.

4. Performance Efficiency

The performance efficiency pillar includes the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve. You can find prescriptive guidance on implementation in the Performance Efficiency Pillar whitepaper.

Design Principles
There are five design principles for performance efficiency in the cloud:

- Democratize advanced technologies
- Go global in minutes
- Use serverless architectures
- Experiment more often
- Mechanical sympathy
- Best Practices
- Take a data-driven approach to selecting a high-performance architecture. Gather data on all aspects of the architecture, from the high-level design to the selection and configuration of resource types.

By reviewing your choices on a cyclical basis, you will ensure you are taking advantage of the continually evolving AWS cloud. Monitoring will ensure you are aware of any deviance from expected performance and can take action on it.

Finally, your architecture can make tradeoffs to improve performance, such as using compression or caching, or relaxing consistency requirements.
The optimal solution for a particular system will vary based on the kind of workload you have, often with multiple approaches combined. Well-architected systems use multiple solutions and enable different features to improve performance.

5. Cost Optimization
The cost optimization pillar includes the ability to avoid or eliminate unneeded cost or suboptimal resources. You can find prescriptive guidance on implementation in the Cost Optimization Pillar whitepaper.

Design Principles
There are five design principles for cost optimization in the cloud:

- Adopt a consumption model
- Measure overall efficiency
- Stop spending money on data center operations
- Analyze and attribute expenditure
- Use managed services to reduce cost of ownership
- Best Practices
- As with the other pillars, there are tradeoffs to consider. For example, do you want to optimize for speed to market or for cost? In some cases, it’s best to optimize for speed—going to market quickly, shipping new features, or simply meeting a deadline—rather than investing in upfront cost optimization.

Design decisions are sometimes guided by haste as opposed to empirical data, as the temptation always exists to overcompensate “just in case” rather than spend time benchmarking for the most cost-optimal deployment. This often leads to drastically over-provisioned and under-optimized deployments.

Using the appropriate instances and resources for your system is key to cost savings. For example, a reporting process might take five hours to run on a smaller server but one hour to run on a larger server that is twice as expensive. Both servers give you the same outcome, but the smaller one will incur more cost over time. A well-architected system will use the most cost-effective resources, which can have a significant and positive economic impact.

Conclusion
The AWS Well-Architected Framework provides architectural best practices across the five pillars for designing and operating reliable, secure, efficient, and cost-effective systems in

the cloud. The framework provides a set of questions that allows you to review an existing or proposed architecture. It also provides a set of AWS best practices for each pillar.

Using the Framework in your architecture helps you produce stable and efficient systems, which allows you to focus on functional requirements. More details on the AWS Well Architected Framework is attached with this technical response.

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.

Response:
Amazon Web Services
The AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). AWS Regions provide multiple, physically separated and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. These Availability Zones offer AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures. For customers who specifically need to replicate their data or applications over greater geographic distances, there are AWS Local Regions. An AWS Local Region is a single datacenter designed to complement an existing AWS Region. Like all AWS Regions, AWS Local Regions are completely isolated from other AWS Regions. The AWS Cloud spans 55 Availability Zones within 18 geographic Regions and one Local Region around the world.

High Availability Through Multiple Availability Zones
Unlike virtually every other technology infrastructure provider, each AWS Region has multiple Availability Zones and data centers. As we've learned from running the leading cloud infrastructure technology platform since 2006, customers who care about the availability and performance of their applications want to deploy these applications across multiple Availability Zones in the same region for fault tolerance and low latency. Availability Zones are connected to each other with fast, private fiber-optic networking, enabling you to easily architect applications that automatically fail-over between Availability Zones without interruption.

For more detailed information: https://aws.amazon.com/about-aws/global-infrastructure/

AWS GovCloud (US) Region

AWS GovCloud (US) is an isolated AWS region, subject to FedRAMP High and Moderate baselines, and it allows customers to host sensitive Controlled Unclassified Information (CUI) and all types of regulated workloads. Availability Zones located within the AWS GovCloud (US) region are physical locations consisting of one or more discrete data centers, each of which has redundant power, networking and connectivity, and is housed in separate facilities. Each Availability Zone (AZ) has multiple Internet connections and power connections to multiple grids. Availability Zones provide customers with additional flexibility to architect scalable, fault-tolerant, and highly available applications in AWS GovCloud (US). The region is operated by employees who are U.S. citizens on U.S. soil. The region is only accessible to vetted U.S. entities and root account holders, who must confirm they are U.S. Persons to gain access to this region.

Druva

Druva runs on Amazon Web Services and uses Amazon S3 for backup storage. This means that it inherits the same redundancy and failover capability that AWS provides.

CloudBerry

Cloudberry runs on Amazon Web Services and gives you the ability to use Amazon S3 for backup storage. This means that the backup storage inherits the same redundancy and failover capability that AWS provides.

Trend Micro

Available when requested..

CloudHealth

CloudHealth runs on Amazon Web Service and ingests data from AWS and other cloud services. The data ingested by CloudHealth is stored in AWS using Amazon S3. This means that the data ingested by CloudHealth inherits the same redundancy and failover capability that AWS provides.

DUO

Duo has maintained uptime of greater than 99.99% for more than four years, with a hard service level guarantee backed by SLA. Duo’s servers are hosted across independent PCI DSS, ISO 27001-certified, and SSAE 16-audited service providers with strong physical security.

DUO provides a high-availability service split across multiple geographic regions, providers and power grids for seamless failover, and our multiple offsite backups of customer data are encrypted.

8.16 (E) HOSTING AND PROVISIONING

8.16.1

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

Response:

Amazon Web Services Management Console

The AWS Management Console facilitates cloud management and provisioning for all aspects of your AWS account, including deploying EC2 instances, accessing monthly spending by service, setting up DynamoDB tables, managing security credentials, setting up new IAM Users and much more. Use the AWS Management Console to explore all available AWS services and perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console is your primary cloud hosting provisioning platform and supports all AWS regions and lets customer’s provision resources across multiple regions.

Command Line Interface

The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Amazon Web Services Management Portal for vCenter Server

AWS Management Portal for vCenter Server enables you to manage your AWS resources using VMware vCenter. The portal installs as a vCenter Server plug-in within your existing vCenter Server environment. Once installed, it enables you to migrate VMware VMs to Amazon EC2 and manage AWS resources from within vCenter Server. AWS resources that you create using AWS Management Portal for vCenter Server will be located in your AWS account, even though they have been created using vCenter Server. For experienced VMware administrators, AWS Management Portal for vCenter Server provides a familiar look-and-feel that will make it easy to start using AWS. For enterprises with existing VMware-based environments, the portal makes it easy to begin moving computing resources to the cloud, while continuing to leverage existing tools and training materials while beginning their transition.

Amazon EC2 VM Import Connector

The new Amazon EC2 VM Import Connector is a virtual appliance (vApp) plug-in for

VMware vCenter. Once installed, you can import virtual machines from your VMware vSphere infrastructure into Amazon EC2 using the GUI that you are already familiar with. The Connector stores separate AWS credentials for each vCenter user so that multiple users (each with separate AWS accounts) can use the same Connector. You can download the Connector from the AWS Developer Tools page. Once the VM has been imported, customers can launch it as an instance from the AWS Management Console and immediately take advantage of all the features of Amazon EC2.

Amazon Web Services Add-ins for Microsoft System Center
AWS add-ins for Microsoft System Center extend the functionality of your existing Microsoft System Center implementation. The add-ins are software that you download and install for use with Microsoft System Center Operations Manager and Microsoft System Center Virtual Machine Manager. After you install the add-ins, you can use the familiar System Center interface to view and manage your Amazon EC2 for Microsoft Windows Server resources within the AWS cloud, as well as Windows Servers installed on-premises.

AWS CloudFormations
AWS CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. This file serves as the single source of truth for your cloud environment. This helps you to standardize infrastructure components used across your organization, enabling configuration compliance and faster troubleshooting. AWS CloudFormation provisions your resources in a safe, repeatable manner, allowing you to build and rebuild your infrastructure and applications, without having to perform manual actions or write custom scripts. CloudFormation takes care of determining the right operations to perform when managing your stack, and rolls back changes automatically if errors are detected.

8.16.2

Provide tool sets at minimum for:

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

Response:
NASPO Participating Entities will be able to deploy all purchased services on-demand 24x365 through the AWS Management Console. The AWS Management Console is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Purchasing Entities can

use the AWS Management Console to perform any number of tasks, from deploying servers to monitoring the health of applications. The AWS Management Console also enables the Purchasing Entity to manage all aspects of their AWS account, including managing security credentials or even setting up new AWS Identity and Access Management (AWS IAM) users. The AWS Management Console supports all AWS regions and lets NASPO customer's provision resources across multiple regions. The Purchasing Entity may also utilize the AWS Command Line Interface (CLI) is a unified tool to deploy and manage AWS services. The CLI services requires one tool to download and configure that can control multiple AWS services from the command line. Additionally, AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS API-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits. Customers can use AWS Software Development Kits (SDK) to programmatically provision or manage IaaS without any interaction with i2m or AWS.

2. Creating and storing server images for future multiple deployments

Response:
Amazon Web Services
i2m uses a AMI/Snapshot scheduling and maintenance tool to create, schedule and manage Amazon Machine Images(AMI) of Amazon EC2 instances and Snapshots of Amazon Block Store(Amazon EBS) volumes in AWS. AMI's are the cloud equivalent to server images. The Purchasing Entity can launch multiple Amazon EC2 instances from a single AMI when you need multiple instances with the same configuration. The Purchasing Entity can also use different AMIs to launch Amazon EC2 instances when they need instances with different configurations. The AMI's and Snapshots are stored in Amazon S3 and are high durable meaning the underlying storage mechanism for the AMIs and snapshots is designed from the ground up to deliver 99.999999999% of durability. Any server hosted in AWS will use this method for image backup.

An AMI includes the following:

- A template for the root volume for the instance (for example, an operating system, an application server, and applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it's launched

CloudBerry

i2m uses Cloudberry's Image-based backup for on-premise servers which allows us to store the state of the system at a certain time. We can store these Server Images onsite or on Amazon S3 or other CSPs. These images can be used for future deployments on-premise or used to create Amazon EC2 instances in AWS, or Azure instances.

Druva

Druva Phoenix enables cloud-based data protection and management for enterprise workloads including physical(file servers and/or NAS and databases), virtual(Microsoft Hyper-V, VMware vSphere, and Nutanix AHV) and hybrid(VMware Cloud on AWS (VMC)) environments. An IT team can easily failover virtual machines (VMs) for DR with a recovery time objective (RTO) of minutes and restore speeds up to 1 TB per hour, as well replicate data or spin up instances cross-region for test and dev(workload mobility) purposes—all on the same platform.

3. Securing additional storage space

Response:

Amazon Web Services

Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Amazon EBS volumes are network-attached, and persist independently from the life of an instance. AWS allows you to dynamically increase capacity, tune performance, and change the type of live EBS volumes to accommodate your storage needs. Additional storage space can be secured through the AWS Management Console or through well-defined and documented Application Programming Interfaces (APIs).

Druva

Druva uses Amazon S3 for storing backups which allows them to provide virtually unlimited storage for each user.

CloudBerry

Cloudberry uses Amazon S3 for storing backups which allows them to provide virtually unlimited storage for each device.

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).

Response:

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications Participating Entities run on AWS. Participating Entities can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. 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 your applications and services, and any log files your applications generate. Participating Entities can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. Participating Entities can use these insights to react and keep your application running smoothly.

Amazon CloudWatch metrics, alarms and logs integrate with a wide variety of popular monitoring platforms like Nagios, DataDog, PagerDuty, and much more.

CloudHealth

CloudHealth enhances user visibility and control of cloud costs, usage, security, and performance. The heightened transparency across any multi-cloud environment drives more informed decision making. Correlate data for analysis and reporting against business objectives. With CloudHealth the Purchasing Entity can create interactive reports across multiple dimensions, time frames, perspectives, groups, or any combination of these. CloudHealth acts as a single pane of glass to better organize, manage, and optimize that ecosystem. By giving you a consolidated view you can better understand how everything works together. The Purchasing Entity can create dashboards and reports to gain visibility of your entire hybrid environment--across all accounts, clouds, departments, and teams regardless of your environment – public cloud, private cloud, or data center.

8.17 (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE)

8.17.1

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

Testing and Training periods may vary dependent on Solutions:

Pre Purchase:

AWS: up to 90 days at AWS monthly spend level below $100/month any charges above $100/month will be charged to Purchase Entity at Cost Proposal rate.

CloudHealth: unlimited admin accounts, 1 complete billing month capture (31 days-62 days)

CloudBerry: unlimited user accounts, max 3 device licenses for 1 month (31 days)

DUO: unlimited admin accounts, max 5 users for 1 month (31 days)

Trend Micro: unlimited admin accounts, max 5 device licenses for 1 month (31 days), on-demand Self-Serve Demo Environment

Druva: unlimited admin accounts, max 3 device licenses for 1 month (31 days)

Post Purchase:

No Testing or demo environments will be provided without cost beyond the limits set above. i2m can migrate certain demo environment to a contract if the entity requests for additional testing and POC. This environment will be on-demand and can be terminated or migrated to a production solution at will of the entity.

Training

Training will provided at any time pre/post purchase according to section 8.18.3 below.

8.17.2

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

Response:

i2m will offer demonstrations of any of its solutions or other value add-on services at no additional cost to the Purchasing Entities. Purchasing Entities may ask i2m to demonstrate its proposed solution, which can be completed remotely free of charge or if requested the solution demonstration be onsite, The Purchasing Entities are charged a pass through rate for any Room/Board and Travel Expenses when performing on-site demonstrations.

8.18.3

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

Response:
Member support and training (initial and ongoing):

Cloud services account(s) retrieval and creation training will be provided for each Members during the initial request for services. 1 hour of initial support and training is included at no additional cost for each member, any hours beyond 1 hour will be billed at rates specified in Cost Proposal within this proposal.

All other ongoing cloud services support and training will also be billed rates specified in

Cost Proposal within this proposal**.**

8.18 (E) INTEGRATION AND CUSTOMIZATION

8.18.1

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

Response:

AWS and the other cloud solutions provided within this proposal use industry standard interfacing techniques, REST and HTTPS API calls and endpoints that interface with the industry standard technologies and protocols. Making it simple to use existing legacy architectures and solutions along with our services offerings.

Integration Protocols:

All service offerings include several supported protocols supported range from web enabled services to traditional Web Services, HTTP, HTTPS, SOAP, XML, JSON CORBA, MQ Series, Sybase OC, RPC, JDBC, ODBC are some examples of current implementations.

LAN/WAN access can be via public or private networks utilizing Internet, AWS Direct Connect, VPN, Frame, ISDN and other network capabilities.

Portability

AWS is popular in the portability and integration of the majority of its services to other cloud providers or even on premise solutions, existing legacy applications and infrastructure and integration with a variety of monitoring tools and solutions. Making it easy for organizations to migrate their solutions between cloud service providers and on premise environments avoiding vendor lock in.

All SaaS solutions integrate between the public, hybrid and private cloud deployment models including on premise deployments. They are also portable and highly integrate with all major cloud services providers; GCP, Azure, IBM and several other service providers. They include features specific meant for several providers to give the consumer the option to choose their service provider of choice or a mix of them as their backend.

Integrations:

Integration services revolve around shared services such as Identity Federation, Monitoring tools integration, database compatibility, code deployment integration, VM compatibility, and DevOps integration.

It is important to understand that the cloud environment deployed on AWS can be treated as a logical extension of your existing datacenters.

If an organization decides to move or migrate to another cloud service provider's infrastructure solution or to create a multi cloud strategy for their organizations, these IaaS, PaaS, SaaS solutions support this natively. These chosen solutions were analyzed and tested by i2m to be highly portable and integrated with existing on premise infrastructure solutions and all major cloud services providers.

8.18.2

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

Response:
Customization
AWS, and SaaS cloud services solutions have many features built in, that allow highly customizable architectures and fine grain features and control within its services suite further mentioned throughout this proposal.

Personalization
All i2m's solutions offer branding and personalization features which give you the option to replace the solution brand with the organization's logos and other supporting personalized information that fit the specific needs of the Purchasing Entity. Below are just some examples other Solution offerings personalization and branding features are available on-demand.

AWS
You can now customize your users' AppStream 2.0 experience with your logo, color, text, and help links in the application catalog page. Using your own brand provides a familiar look and feel when users access your applications. Adding your own help links makes it easy for them to access support resources within your organization.

You can customize your branding for no additional charge in all AWS Regions where AppStream 2.0 is offered. AppStream 2.0 offers pay-as-you-go pricing. Please see Amazon AppStream 2.0 Pricing for more information, and try our sample applications.

AWS Service Catalog, used by enterprises, system integrators, and managed service providers to organize, govern, provision, and operate cloud resources on AWS, now allows customers to customize the look and feel of the console. Customers can brand their AWS Service Catalog console to match their internal applications, making the user experience more seamless when moving from internal applications such as single sign-on and navigation portals to AWS Service Catalog.

AWS Service Catalog administrators can change the logo and color specifications to reflect their desired console branding. They have the flexibility to upload a logo in PNG, JPG, or SVG image file formats. Administrators can also choose a primary and accent color for other site components using a color picker or RGB color value.

CloudBerry:
White-Label Cloud Backup
Rebrand and customize the backup client so it's fully aligned with your own company's style and brand identity. With CloudBerry backup software you can replace everything from logos and images to email address and website link.

- Rebranding the Splash screen of CloudBerry white-label online backup software
- Rename the product
- Replace all banners and logos
- Your contact email address
- Use your icons (main and tray)
- Put your contact details
- Control panel under your domain (hosted SSL certificate)
- Insert your company name
- Replace splash screen
- Your welcome text on startup
- Place link to your website
- Use your support email address
- Replace copyright text
- White-label control panel
- Online Access with your domain

8.19 (E) MARKETING PLAN

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

Response:
Summary of Marketing Plan:

The Strategy is to create ourselves an online presence by using our website http://i2m.cloud and NASPO ValuePoint website and resources as a general brochure, menu of services, and call to action to see and demo our cloud solutions services offerings. Creating a newsletter periodically with marketing material to send to potential Purchasing Entities or Contracted Entities. This marketing material will contain either helpful technical services articles, services updates and new solutions available by AWS and other Cloud Service Providers offerings along with i2m's value-add services and implementation services. i2m will utilize AWS Marketing Central a sales and marketing platform with targeted campaigns for the AWSs Public Sector with campaigns and contents for AWS IaaS, PaaS and SaaS solutions offerings. We also have campaign partnerships with the remaining SaaS solutions offered which we will utilize alongside our own campaign platform to keep our contracted Entities informed. i2m will ask approval of NASPO ValuePoint and Purchasing Entity before any information is sent. This will comply with all the rules and regulations defined in this proposal.

We want to attract organizations to our website for searches like managed cloud services, managed cloud solutions providers, software as a service, cloud migration services, cloud solution providers, IaaS, SaaS and DR. We are ahead in the technology, technical expertise, with real experiences, real customers, and we have proven track record with our clients. We act as a differentiator, between, other cloud MSP's and Resellers we are focused on our client success through bringing them a more robust and affordable cloud solutions and delivering an all-in one solution without having to go to other vendors for their technology stack. We have the tools/software/know how to get them running all from one cloud MSP i2m.

Our website is geared to more easily defined read for all types of viewers; newbies, CEOs and CTOs and Technical Professionals. In essence we strive to be the standard of the cloud managed services market (an assembly line at all levels of design, migration, implementation including support, management, DevOps, optimization). We execute projects with maximum care, efficiency, speed, while simplifying cloud services delivery.

Key Offerings i2m:

AWS (IaaS, PaaS and SaaS) services

i2m makes it affordable and efficient to migrate or start your business on the cloud. With cloud infrastructure:

- You get built-in high availability, scalability, and disaster recovery.
- You can decouple your computing environment from your physical location to isolate the risk of failing or aging on-site equipment and natural disaster.
- You avoid the high capital expenditures of acquiring, replacing and upgrading equipment and software.

You can focus on your core business, and not the physical systems that run it.

Our certified AWS Engineers will work with your team to explain all the benefits that a cloud platform can offer your business. Whether you are looking to tip toe into cloud technologies or are ready to migrate your entire infrastructure, we can guide you through the planning and execution of a successful project.

We offer a broad set of services tailored to your specific needs. We offer complete public, private and hybrid cloud solutions as well as a comprehensive set of management services and performance monitoring.

SaaS

Software sold as a subscription pay monthly for expensive software, cancel when you do need. All the essential software for your business.

We are offer the very core most popular business applications through the various partnerships and reseller associations, we resell all of our cloud software as a service as low easy competitive MSRP prices. Options include Druva, CloudBerry, Trend Micro, CloudHealth . Added advantage all on one bill, managed support for the product.

Disaster Recovery

When Disaster Strikes be able to operate like it never happened do not lose money with outages.

We have plans that align with AWS Best Practice Pilot light, Warm Standby and Multi-Site disaster recovery plans each with their own RTO and RPO values. Each Disaster Recovery Plan is a Custom plan proposed to the business. Every plan is catered to fit budget and essential Business functions. Goal is to make Disaster Recovery affordable and effective, where it wasn’t before cloud services.

Cloud Backup/Storage

i2m backup solutions, have the highest durability at the lowest rate. Very affordable compared to other enterprise solutions.

i2m backup solutions can achieve almost unlimited scalability and is gentle on your systems and network resources. With a notably small memory footprint, it can leverage the full capacity of your infrastructure cloud and on premise. Enterprises of any size now have a certified enterprise-class scalable network backup solution as a realistic alternative to proprietary offerings.

i2m backup solutions balance innovation with enterprise class stability, bringing modern, highly scalable backup and restore to your business. Thousands of organizations worldwide have adopted these service in mission-critical environments thanks to its modern, modular and multi-threaded design.

Marketing Director and Team

The marketing director will execute, marketing campaigns, via AWS Marketing Central he we will search for local marketing/IT/Cloud Services events spreading the word directing people to our web-site giving answering questions related to cloud migration and starting a business in the cloud. Sending bi-monthly/monthly newsletters with offerings to existing/new prospect and new lead clients. This is also going to be the driver to get us better marketing tools, or marketing resources to evaluate what online/local sales/marketing/advertising firms can do for us, like get us quotes, setup online meetings, build a Leads contacts list etc.

Marketing Associates

They will take care of event setup/breakdown/distributing content and overall action items assistant to the marketing director if/when needed. This comes later in a few months.

Marketing Director

Will handle vision items like how a new technology is sellable/marketable, relaying feedback to management and i2m partners and AWS and SaaS partner team, Will be working closely to the marketing team to train them on what to sell, how to sell, what markets to tap, who the need to get the message too. Set goals and expectancy of the marketing. They will require i2m management approval for any operations that will then filter to NASPO ValuePoint and Purchasing Entity for approval.

Duties and Roles

- Will be meeting with Sales/Marketing Managers and working on projects/evaluating results, preparing for AWS and SaaS Partners cloud campaigns.
- Will relay all AWS/i2m.cloud updates in a meeting physical/virtual i2m staff, sales/marketing managers and Purchaisng Entities and NASPO.
- Bi-monthly updates to facebook, twitter, social media, i2m.cloud blog contents: technical articles, customer success stories, how to's, promotional offers, promotional events and other marketing and sales digital activities.

Online Sales/Marketing Advertising Tools/Services

- AWS Marketing Central free already signed up and ran a few campaigns. Plan to start more campaigns associated with Public sector as well continuing private sector campaigns
- We have been using ConnectWise Sell https://www.connectwise.com/software/sell
- Some other marketing and advertising services i2m uses:

  https://www.adroll.com/

  http://www.hubspot.com/

  http://www.marketo.com/

http://www.yesware.com/

Website Revamp/Additions:

i2m website is in midst of revamp to include and highlight the Public Sector specific services offerings.

i2m Marketing Events:

- AWS joint webinars and joint sales/marketing events
- SaaS offerings and partners joint webinars and joint sales/marketing events

Marketing Guidelines i2m follows:

1. USE AWS MARKETING ALONG WITH AWS PARTNER MARKETING TOOLS PROVIDED

2. USE our CRM TOOL FOR CUSTOMERS

3. START BUILDING EMAIL LIST

4. DISTRIBUTE PRESS RELEASE ONCE A QUARTER

Press releases are easy to create and can be promotional in nature. The editorial guidelines are straightforward and it is easy to get your releases accepted on major press release distribution sites. It is an easy way to market your business and boost your online visibility. For best results, contact local media including newspapers and magazines to see if they will publish your press release. You may be surprised with the result.

5. TAKE STEPS TO BOOST CONVERSIONS

There are many small businesses that get a lot of traffic on their website but fail to convert them into leads. Your website traffic is of little use if you cannot convert them into customers for your business. There are many ways to do this. Here are some examples:

- Use good call to action on website
- Use call to action in all other marketing material
- Make sure call to action are prominently displayed throughout your website

6. LEARN FROM OTHER BUSINESSES

We can learn a lot from other successful businesses in our niche. Simply looking at their website and social profiles can tell you a lot. There are also many competitive analysis tools that our business can take advantage of. We research our competition to get inspiration and learn new ways to market our business.

7. OFFER DISCOUNTS AND DEALS

Every consumer loves a discount. Offering discounts and deals are a great way to market your business and reward customers. Make sure to promote your offers on your social media profiles and through articles and blog posts. There are also many deal websites that you can take advantage of. This is a great way to get extra coverage for your business. This will mostly be for SAAS offerings. Deals/Discounts are mostly made during Negations.

9. START USING VIDEOS TO MARKET YOUR BUSINESS

Videos are very popular with consumers today and offer an excellent way to market your business. There are many ways a small business can use videos as part of their marketing strategy.

Displaying product videos on website is a very effective way to increase sales. Studies show that customers are much more likely to buy if they see a video on your product or service landing pages.

Being active on YouTube is another effective way to market your small business. YouTube is one of the most widely used channels by consumers today and building your company’s presence on the site can get extra coverage for your business and help to attract new customers.

You can also start your own YouTube channel to post your videos as well as share videos of other users that are relevant to your target market. Commenting on videos relevant to your niche is another way to engage with users and increase your brand visibility.

If you are creating your own videos, don’t limit yourself to promotional videos about your products or services only. Creating instructional videos that can help your targeted audience to solve common problems will get far more coverage than promotional videos.

We are getting YouTube channel started.

10. HAVE AN ONGOING OPTIMISATION STRATEGY

Your website will be of little use if no one can find it on search engines. Simply optimizing your website at the start is not enough. To get good coverage on search engines, you will need to work on your website continuously, monitoring your statistics closely and refining your website accordingly. You will also need to update your site frequently with keyword rich content and work on building quality back-links to your site.

11. LIST YOUR BUSINESS ON POPULAR LOCAL DIRECTORIES

Other local business directories such as Google Plus Local, Bing Local and Yahoo Local are equally important. Make sure to include a good description about your business and a link to your website.

11. LIST YOUR BUSINESS ON LOCATION BASED SERVICES AND APPS

Location based services such as Yelp and foursquare are very popular among consumers. Listing your business on these services is a great way to market your business and attract new customers.

13. BE ACTIVE ON SOCIAL MEDIA

A majority of small business already have a profile on the main social networks such as Facebook and Twitter. But this in itself will not offer much marketing benefits for your business. To maximize the benefits of social media, you must do more. Here are some tips:

- Keep your profiles up to date and fresh with new information
- Post few times per week
- Add value for users by sharing content that is of value to them
- Engage actively with users – follow, share, retweet, like content of other users
- Don’t just share content from your website

14. TRY GOOGLE ADWORDS

Google Adwords, Google’s paid advertising program, is a very effective way to get your website listed on search engines for your desired search terms. It can be very effective particularly in the short term while you work on improving your organic rank in the free listings. Due to increasing competition, the cost per click can be high but you can set a maximum monthly budget to keep your costs in control. With the right targeting, the ROI can be easily noticeable.

You can also use free advertising vouchers to try it out and get some advertising for your business for free.

15. CONSIDER PAID ADVERTISING ON SOCIAL MEDIA

If you are new and do not yet have a large enough following on social media, you can consider paid advertising on social media. Social networks like Twitter, Facebook and YouTube offer cost-effective advertising options for businesses.

17. LEVERAGE CONTENT MARKETING

Content marketing i.e. producing and distributing quality content that is relevant to your audience is one of the most effective ways to market your business and attract customers. This form of marketing is also highly targeted. If done correctly, content marketing can prove a very valuable asset to your marketing strategy. For best results, product a variety content types such as articles, infographics, videos, or webinars and distribute them on several channels.

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.

i2m specific value-added services and capabilities:

Cloud Services:

- Infrastructure as a Service (IaaS) Initial Setup, Delivery and Management
- Managed Windows Active Directory in the Cloud
- Microsoft Workloads and Application delivery and management
- Remote App and Remote Desktop Services delivery on AWS
- Managed Cloud Desktops (DaaS)
- Managed Software as a Service (SaaS)
- Managed Platform as a Service (PaaS) solutions on AWS
- Managed Disaster Recovery (DRaaS)
- Enterprise Class Cloud Backup and Recovery Services
- Cloud Migration and Optimization Services
- Cloud Governance, Security, Reporting and Analytics Services
- High Availability and Fault Tolerant Design and Build Services
- DevOps/SysOps Services
- Cloud Security Optimization

- 24×7 Predictive Monitoring and Proactive Support Services
- Public Sector Cloud Services for Cities, States, Governments, and Non-Profits
- Cloud Authentication and Authorization Services (SSO)
- Training
- One Vendor, One Bill for all your Cloud Services

Management Services:

- Server Management and Desktop/User Support and Optimization
- Preventative Maintenance
- Critical Patch Management
- Help Desk Support
- Onsite Support
- Secure Remote Support
- Problem Isolation and Resolution
- How To? Questions Answered
- Managed Local, Endpoint and Enterprise Backup and Disaster Recovery
- Managed e-mail (Private or Shared) with Spam/Virus Protection
- Managed Web Hosting
- Managed Virus Protection
- Microsoft Office 365 Implementation
- Training
- Technology Consulting

Network Services:

- LAN/WAN Management
- Network Edge, Router, Firewall and Telecom Management
- VoIP Implementations
- Network Audits
- Migration Planning
- Network Operations Center
- Network System Integration Services
- Network Consulting Services
- Project Management and General Technology Consulting

8.22 (E) SUPPORTING INFRASTRUCTURE

8.22.1

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

Response:

There is no specific infrastructure that is required outright by i2m to support our solutions/services offered. Participating Entities can choose the infrastructure of choice to implement using hybrid and private deployments models. i2m can recommend specific infrastructure that has been tested and evaluated by i2m for operational efficiency and stability. At minimum Purchasing Entities will require an Internet Connection to access API calls and Web Consoles of solutions offered. For private connectivity to AWS either the use of a VPN Firewall that's supports IP SEC, VPN Software client to connect to a VPN Server at AWS or a direct connection to AWS using Ethernet services like AWS Direct Connect for a dedicated and more robust connection.

8.22.2

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

Response:

The purchasing entity can choose to install any new infrastructure themselves. Optionally i2m can co-conduct or lead the installation of new infrastructure/hardware. Any assistance that is required from i2m during installation will be expensed at our onsite or remote installation hourly rates specified in our Cost Proposal.

AWS Solution Provider Program
Program Guide for End Customers

Last updated: 07/02/2018

1. Solution Provider Program Overview

The Solution Provider Program lets you take advantage of authorized systems integrators, managed service providers, and value-added resellers ("**Authorized Solution Providers**") who provide integrated solutions combining one or more products or services they offer with a subset of Services ("**Authorized Services**", and such combinations, "**Solutions**") and likely have attended AWS technical trainings, established AWS expertise, created a program based on AWS services, and trained their sales team on AWS services. Your Authorized Solution Provider (with your consent) can manage your AWS accounts on your behalf and will be your point of contact, including for services, support, pricing and billing, for such accounts.

Capitalized terms have the meanings set forth in the AWS Customer Agreement available at http://aws.amazon.com/agreement by and between Amazon Web Services, Inc. and its affiliates and you, or other written agreement between us and you governing your access to and use of Authorized Services ("**Services Agreement**") or the Service Terms (as defined in the Services Agreement) unless otherwise defined in this Program Guide. This Program Guide is available at https://s3-us-west-2.amazonaws.com/solution-provider-program-legal-documents/AWS+Solution+Provider+Program+-+Program+Guide+for+End+Customers.pdf and may be updated by AWS from time to time.

2. Access to and Use of Authorized Services

In order for your Authorized Solution Provider to provide the Authorized Services to you on your own AWS accounts, you must have a Services Agreement in place and give your Authorized Solution Provider access to such AWS accounts (as further described below) as your subcontractor or agent. Because these accounts are your AWS accounts, your Services Agreement will govern all access to and use of the Services on such accounts, except for fees, payment, pricing, and tax terms for your use of the Services, which are superseded by such terms in your agreement with your Authorized Solution Provider. You will receive your invoice from and pay your Authorized Solution Provider for your use of the Solutions, as well as your use of any other Services on the accounts.

3. Program Account Creation

Before giving your Authorized Solution Provider access to your AWS accounts for purposes of the Solution Provider Program, ensure your AWS account is in your own (full legal) name using your email address (with an email domain owned by you). If you don't already have an AWS account, you can create the AWS account yourself or your Authorized Solution Provider (or other entity from whom your Authorized Solution Provider directly or indirectly purchased the Authorized Services) can assign an AWS account to you (with AWS's consent).

To transition your AWS account from a direct account with AWS to an account in the Solution Provider Program, (a) you must join the account to the Master Account specified by your Authorized Solution Provider using AWS Organizations (or any successor or related Service designated by AWS), and (b) for the account, the Tax Settings page in the console must be updated to your Authorized Solution Provider's tax settings, including business legal address, tax registration number, and business legal name (if applicable) or if directed pursuant to the Tax Settings page, the Payment Methods page in the console must be updated to your Authorized Solution Provider's billing information, including billing address. You can transition additional AWS accounts from direct accounts with AWS to accounts in the Solution Provider Program in the same way, or you can authorize your Authorized Solution Provider (or other entity from whom your Authorized Solution Provider directly or indirectly purchased the Authorized Services) in writing to create AWS accounts on your behalf.

If your Authorized Solution Provider (or other entity from whom your AWS Authorized Solution Provider directly or indirectly purchased the Authorized Services) creates AWS accounts on your behalf (with your written consent), you should request the root user credentials at the time the accounts are created. AWS does not disclose root user credentials and cannot release those credentials to you. For a list of tasks that require root user credentials, please visit https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html (or any successor or related location designated by AWS, as may be updated by AWS from time to time).

If you have any special arrangements with AWS with respect to any AWS accounts that you intend to transition from a direct account with AWS to an account in the Solution Provider Program, contact your current AWS account manager to discuss any potential implications on your special arrangement.

4. Authorized Solution Provider Access

There are two operating modes within AWS Organizations: Consolidated Billing and All Features. Before you join your AWS accounts to the Master Account specified by your Authorized Solution Provider, you should work with your Authorized Solution Provider to determine which mode is best for you.

If Consolidated Billing is enabled, only your usage and invoices are made available to your Authorized Solution Provider. You can then use AWS Identity and Access Management to manage your Authorized Solution Provider's access to your AWS account, AWS resources, and the Services. For guidance and best practices, visit https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html (or any successor or related location designated by AWS, as may be updated by AWS from time to time).

If All Features is enabled, your usage and invoices are made available to your Authorized Solution Provider, and your Authorized Solution Provider (and, if applicable, the third-party entity from whom your Authorized Solution Provider directly or indirectly purchased the Authorized Services) will have full control over what your AWS accounts can do. Additionally, through AWS Single Sign-On integration with AWS Organizations, your Authorized Solution Provider (and such other entity) may also have access to your Content.

If you allow your Authorized Solution Provider to collect, use, transfer, disclose, and otherwise process your Content or Account Information, including personal data, you should familiarize yourself with your Authorized Solution Provider's relevant privacy practices, which may differ from AWS's privacy practices.

Note that in accordance with the AWS Organizations user guide, once All Features mode is enabled, you cannot revert to Consolidated Billing mode. To access a copy of the AWS Organizations user guide, visit https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html (or any successor or related location designated by AWS, as may be updated by AWS from time to time).

5. Authorized Services

If you purchase AWS Managed Services from your Authorized Solution Provider, you may disclose confidentially to your Authorized Solution Provider the AWS Managed Services Addendum between you and us.

6. AWS and Authorized Solution Provider Relationship

Your Authorized Solution Provider and its affiliates are not agents of AWS for any purpose and do not have the authority to bind AWS.

7. Leaving Your Authorized Solution Provider

If you choose to leave your Authorized Solution Provider, (a) you must unjoin your AWS accounts from the Master Account specified by the Authorized Solution Provider you are leaving, and (b) for the account, the Tax Settings page in the console must be updated to your tax settings, including business legal address, tax registration number, and business legal name (if applicable) or if directed pursuant to the Tax Settings page, the Payment Methods page in the console must be updated to your billing information, including billing address. You should consult your agreement with your Authorized Solution Provider to determine the implications of leaving that relationship.

Amazon Web Services (AWS) http://aws.amazon.com/agreement

https://aws.amazon.com/legal/service-level-agreements/

AWS Service Level Agreements

- Amazon API Gateway Service Level Agreement
- Amazon CloudFront Service Level Agreement
- AWS CloudHSM Service Level Agreement
- Amazon Cognito Service Level Agreement
- Amazon Database Migration Service Level Agreement
- AWS Direct Connect Service Level Agreement
- AWS Directory Service Service Level Agreement
- Amazon DocumentDB (with MongoDB compatibility) Service Level Agreement
- Amazon DynamoDB Service Level Agreement
- Amazon EC2 Service Level Agreement
- Amazon EFS Service Level Agreement
- Amazon EKS Service Level Agreement
- Amazon Elastic Container Registry Service Level Agreement
- Amazon Elastic Load Balancing Service Level Agreement
- Amazon ElastiCache Service Level Agreement
- Amazon EMR Service Level Agreement
- Amazon FSx Service Level Agreement
- AWS Glue Service Level Agreement
- AWS Hybrid Storage and Data Transfer Service Level Agreement
- AWS IoT Greengrass Service Level Agreement
- AWS IoT Core Service Level Agreement

- AWS IoT Device Management Service Level Agreement
- AWS Key Management Service Service Level Agreement
- Amazon Kinesis Data Streams Service Level Agreement
- Amazon Kinesis Data Firehose Service Level Agreement
- Amazon Kinesis Video Streams Service Level Agreement
- AWS Lambda Service Level Agreement
- Amazon Messaging (SQS, SNS) Service Level Agreement
- Amazon MQ Service Level Agreement
- Amazon RDS Service Level Agreement
- Amazon Rekognition Service Level Agreement
- Amazon Route 53 Service Level Agreement
- Amazon S3 Service Level Agreement
- Amazon SageMaker Service Level Agreement
- AWS Secrets Manager Service Level Agreement
- AWS Shield Advanced Service Level Agreement
- Amazon Simple Workflow Service Level Agreement
- AWS Step Functions Service Level Agreement
- Amazon Storage Gateway Service Level Agreement
- AWS WAF Service Level Agreement

Terms and Conditions

> Company > Legal Information > Terms and Conditions

CloudBerry Lab Terms and Conditions

This document was last updated on December 12, 2017

These terms and conditions ("Terms", "Agreement") are an agreement between CloudBerry Lab ("CloudBerry Lab", "us", "we" or "our") and you ("User", "you" or "your"). This Agreement sets forth the general terms and conditions of your use of the https://www.cloudberrylab.com website and any of its products or services (collectively, "Website" or "Services").

Accounts and membership

If you create an account on the Website, you are responsible for maintaining the security of your account and you are fully responsible for all activities that occur under the account and any other actions taken in connection with it. Providing false contact information of any kind may result in the termination of your account. You must immediately notify us of any unauthorized uses of your account or any other breaches of security. We will not be liable for any acts or omissions by you, including any damages of any kind incurred as a result of such acts or omissions. We may suspend, disable, or delete your account (or any part thereof) if we determine that you have violated any provision of this Agreement or that your conduct or content would tend to damage our reputation and goodwill. If we delete your account for the foregoing reasons, you may not re-register for the our Services. We may block your email address and Internet protocol address to prevent further registration.

Billing and payments

You shall pay all fees or charges to your account in accordance with the fees, charges, and billing terms in effect at the time a fee or charge is due and payable. Where Services are offered on a free trial basis, payment may be required after free trial period ends, and not when you enter your billing details (which may be required prior to the commencement of the free trial period). If auto-renewal is enabled for the Services you have subscribed for, you will be charged automatically in accordance with the term you selected. If, in our judgment, your purchase constitutes a high risk transaction, we will require you to provide us with a copy of your valid government-issued photo identification, and possibly a copy of a recent bank statement for the credit or debit card used for the purchase. We reserve the right to change products and product pricing at any time. We also reserve the right to refuse any order you place with us. We may, in our sole discretion, limit or cancel quantities purchased per person, per household or per order. These restrictions may include orders placed by or under the same customer account, the same credit card, and/or orders that use the same billing and/or shipping address. In the event that we make a change to or cancel an order, we may attempt to notify you by contacting the e-mail and/or billing address/phone number provided at the time the order was made.

Accuracy of information

Occasionally there may be information on the Website that contains typographical errors, inaccuracies or omissions that may relate to pricing, promotions and offers. We reserve the right to correct any errors, inaccuracies or omissions, and to change or update information or cancel orders if any information on the Website or on any related Service is inaccurate at any time without prior notice (including after you have submitted your order). We undertake no obligation to update, amend or clarify information on the Website including, without limitation, pricing information, except as required by law. No specified update or refresh date applied on the Website should be taken to indicate that all information on the Website or on any related Service has been modified or updated.

caused by you or your activities; (3) outages that do not affect core Service functionality; (4) causes beyond our control or that are not reasonably foreseeable; and (5) outages related to the reliability of certain programming environments.

Backups

We are not responsible for Content residing on the Website. In no event shall we be held liable for any loss of any Content. It is your sole responsibility to maintain appropriate backup of your Content. Notwithstanding the foregoing, on some occasions and in certain circumstances, with absolutely no obligation, we may be able to restore some or all of your data that has been deleted as of a certain date and time when we may have backed up data for our own purposes. We make no guarantee that the data you need will be available.

Prohibited uses

In addition to other terms as set forth in the Agreement, you are prohibited from using the Website or its Content: (a) for any unlawful purpose; (b) to solicit others to perform or participate in any unlawful acts; (c) to violate any international, federal, provincial or state regulations, rules, laws, or local ordinances; (d) to infringe upon or violate our intellectual property rights or the intellectual property rights of others; (e) to harass, abuse, insult, harm, defame, slander, disparage, intimidate, or discriminate based on gender, sexual orientation, religion, ethnicity, race, age, national origin, or disability; (f) to submit false or misleading information; (g) to upload or transmit viruses or any other type of malicious code that will or may be used in any way that will affect the functionality or operation of the Service or of any related website, other websites, or the Internet; (h) to collect or track the personal information of others; (i) to spam, phish, pharm, pretext, spider, crawl, or scrape; (j) for any obscene or immoral purpose; or (k) to interfere with or circumvent the security features of the Service or any related website, other websites, or the Internet. We reserve the right to terminate your use of the Service or any related website for violating any of the prohibited uses.

Intellectual property rights

This Agreement does not transfer from CloudBerry Lab to you any CloudBerry Lab or third-party intellectual property, and all right, title, and interest in and to such property will remain (as between the parties) solely with CloudBerry Lab. All trademarks, service marks, graphics and logos used in connection with our Website or Services, are trademarks or registered trademarks of CloudBerry Lab or CloudBerry Lab licensors. Other trademarks, service marks, graphics and logos used in connection with our Website or Services may be the trademarks of other third parties. Your use of our Website and Services grants you no right or license to reproduce or otherwise use any CloudBerry Lab or third-party trademarks.

Disclaimer of warranty

You agree that your use of our Website or Services is solely at your own risk. You agree that such Service is provided on an "as is" and "as available" basis. We expressly disclaim all warranties of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and non-infringement. We make no warranty that the Services will meet your requirements, or that the Service will be uninterrupted, timely, secure, or error free; nor do we make any warranty as to the results that may be obtained from the use of the Service or as to the accuracy or reliability of any information obtained through the Service or that defects in the Service will be corrected. You understand and agree that any material and/or data downloaded or otherwise obtained through the use of Service is done at your own discretion and risk and that you will be solely responsible for any damage to your computer system or loss of data that results from the download of such material and/or data. We make no warranty regarding any goods or services purchased or obtained through the Service or any transactions entered into through the Service. No advice or information, whether oral or written, obtained by you from us or through the Service shall create any warranty not expressly made herein.

Limitation of liability

To the fullest extent permitted by applicable law, in no event will CloudBerry Lab, its affiliates, officers, directors, employees, agents, suppliers or licensors be liable to any person for (a): any indirect, incidental, special, punitive, cover or consequential damages (including, without limitation, damages for lost profits, revenue, sales, goodwill, use or content, impact on business, business interruption, loss of anticipated savings, loss of business opportunity) however caused, under any theory of liability, including, without limitation, contract, tort, warranty, breach of statutory duty, negligence or otherwise, even if CloudBerry Lab has been advised as to the possibility of such damages or could have foreseen such damages. To the maximum extent permitted by applicable law, the aggregate liability of CloudBerry Lab and its affiliates, officers, employees, agents, suppliers and licensors, You agree to indemnify and hold CloudBerry Lab and its affiliates, directors, officers, employees, and agents harmless from and against any liabilities, losses, damages or costs, including reasonable attorneys' fees, incurred in connection with or arising from any third-party allegations, claims, actions, disputes, or demands asserted against any of them as a result of or relating to your Content, your use of the Website or Services or any willful misconduct on your part.

Severability

All rights and restrictions contained in this Agreement may be exercised and shall be applicable and binding only to the extent that they do not violate any applicable laws and are intended to be limited to the extent necessary so that they will not render this Agreement illegal, invalid or unenforceable. If any provision or portion of any provision of this Agreement shall be held to be illegal, invalid or unenforceable by a court of competent jurisdiction, it is the intention of the parties that the remaining provisions or portions thereof shall constitute their agreement with respect to the subject matter hereof, and all such remaining provisions or portions thereof shall remain in full force and effect.

Dispute resolution

The formation, interpretation and performance of this Agreement and any disputes arising out of it shall be governed by the substantive and procedural laws of California, United States without regard to its rules on conflicts or choice of law and, to the extent applicable, the laws of United States. The exclusive jurisdiction and venue for actions related to the subject matter hereof shall be the state and federal courts located in California, United States, and you hereby submit to the personal jurisdiction of such courts. You hereby waive any right to a jury trial in any proceeding arising out of or related to this Agreement. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement.

Assignment

You may not assign, resell, sub-license or otherwise transfer or delegate any of your rights or obligations hereunder, in whole or in part, without our prior written consent, which consent shall be at our own sole discretion and without obligation; any such assignment or transfer shall be null and void. We are is free to assign any of its rights or obligations hereunder, in whole or in part, to any third-party as part of the sale of all or substantially all of its assets or stock or as part of a merger.

Changes and amendments

We reserve the right to modify this Agreement or its policies relating to the Website or Services at any time, effective upon posting of an updated version of this Agreement on the Website. When we do we will revise the updated date at the bottom of this page. Continued use of the Website after any such changes shall constitute your consent to such changes.

Acceptance of these terms

You acknowledge that you have read this Agreement and agree to all its terms and conditions. By using the Website or its Services you agree to be bound by this Agreement. If you do not agree to abide by the terms of this Agreement, you are not authorized to use or access the Website and its Services.

Contacting us

If you have any questions about this Agreement, please contact us.

CLOUDBERRY MANAGED BACKUP SERVICE AGREEMENT

PLEASE READ THIS SERVICE AGREEMENT CAREFULLY. BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE OR SERVICE YOU INDICATE ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE OR SERVICE. THIS AGREEMENT DOES NOT SUPERSEDE ANY OTHER WRITTEN AGREEMENT BETWEEN YOU AND CLOUDBERRY LAB.

This agreement (the "Agreement") is made between CloudBerry Lab, ("Company") and you, the customer ("Customer"). The terms and conditions of this Agreement are intended by the parties as a final expression of their agreement with respect to the subject matter hereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any judicial proceeding that may involve the Agreement. This Agreement contains, among other things, warranty disclaimers, liability limitations, use limitations and a binding arbitration clause.

This Agreement sets forth the terms under which the Company will provide Customer with access to and use of a certain software-as-a-service SaaS offering known as the CloudBerry Managed Backup Service ("Subscription Service") which provides Customers with managed online backup services under their own brand with access to Cloud Storage Providers ("CSP") of Customer's choosing. With the exception of management and administration data like, but not limited to, usernames, login credentials, email addresses, and computer names created by Customer in order to access the Subscription Service, the Subscription Service has no access to and does not store any of the Customer Data or Customer Content (collectively the "Data") of any kind. Rather, the Subscription Service transfers the Data which is contained in Backup Storage to a ("CSP") of Customer's choosing and / or storage under the control of the customer.

By clicking on this box, the authorized employee executing this agreement on behalf of Customer represents and warrants that he or she has the power and authority to enter into this Agreement and bind Customer to the terms of this Agreement. IF CUSTOMER AGREES TO BE BOUND BY ALL THE TERMS OF THIS AGREEMENT, PLEASE ACCEPT THE AGREEMENT AND PROCEED TO ACCESS THE SUBSCRIPTION SERVICE. IF CUSTOMER DOES NOT AGREE TO BE BOUND BY ALL THE TERMS OF THIS AGREEMENT, COMPANY IS UNWILLING TO GRANT CUSTOMER ANY RIGHTS TO USE THE SUBSCRIPTION SERVICE, AND CUSTOMER MUST STOP ACCESSING THE SUBSCRIPTION SERVICE.

1. Definitions

"**3rd Party**" or **"3rd Parties"** means any person or entity not employed by Company.

"Administrator Users" means the Authorized User(s) designated by Customer who are responsible for administering the Subscription Service and who are issued an Administrator login by Company or Customer.

"Agreement" means these terms and conditions, the Exhibits attached hereto and any other statements of work, exhibits or appendices thereto, whether attached or incorporated by reference.

"Authorized Users" means individuals who are authorized by Customer to use the Subscription Service, for whom subscriptions to a Subscription Service have been purchased and who have been supplied user identifications and passwords by Customer.

"Backup Storage" means any local or cloud storage created by Customer that is not offered by the Company nor maintained or stored by the Subscription Service.

"Customer" means the customer entity that has accepted this Agreement and is authorized to use the Subscription Service.

"Customer Data" or **"Customer Content" (Collectively the "Data")** means all electronic data or information of any kind that Customer (or its authorized users including administrative users, employees, managers, manager users, and 3rd parties regardless of whether or not the Customer Data is owned by Customer during the Term) inputs into Backup Storage that is transferred by the Company via the Subscription Service to a CSP of Customer's choosing and / or storage under the control of the customer. Data includes: (i) Customer records, business documents and files, data files, input materials, reports, forms and other such items that may be transferred by Company, in the performance of the Subscription Service under this Agreement; (ii) Any Data not owned by Customer such as the Data of one of Customer's clients or a 3rd party that Customer is doing business with; or (iii) any information relating to an identified or identifiable natural person including a 3rd party defined as an identifiable person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. This includes administrative users, authorized users, and 3rd parties. Data may include name, email addresses, telephone numbers, information related to logging in to the Services, birth dates, social security numbers, and personally identifiable information (PII) including financial information, and protected health information covered under HIPAA. All Data has been designed, created and provided solely by Customer or by 3rd parties on its behalf without the participation or involvement of Company. Customer shall have the sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness of and copyright, trademark and patent permissions for all Data entered into a Backup Storage. Customer shall not place nor cause to be placed into any Backup Storage any Content or Data that contains any content or materials which is obscene, threatening, malicious, which infringe on or violate any applicable law or regulation or any proprietary, contract, moral, privacy or other third party right, or which otherwise exposes Company to civil or criminal liability. Company assumes no responsibility for the accuracy, propriety, or usefulness to Customer of the Data. Company shall not be liable to Customer or any third-parties for any loss, damage or expense whatsoever and howsoever arising from any Data inputted or entered into Backup Storage by Customer or by an entity on its behalf. Customer acknowledges that the Company will rely on the accuracy of the Data inputted into Backup Storage by Customer as it performs its requested functions under this Agreement. Customer acknowledges that it owns all of the Data or has all rights to grant such licenses to Company to use the Data in furtherance of providing the Subscription Service without infringement or violation of any third party rights. Company provides no warranties, representations or indemnification to Customer for its access to, and use of the Data.

"Electronic Communications" means any information transmitted in whole or part, electronically received and/or transmitted through the Subscription Service.

"Term" has the meaning set forth in Section 10.1 below.

"Third Party Integrated Services" means applications or services that are provided and managed by third party providers, and interoperate with the Subscription Service including but not limited to any third party that enables the Subscription Service to act as a conduit to send Customer Data or any type of information to the intended party.

In consideration for Customer's acceptance of and subject to the terms and conditions incorporated herein and the Privacy Policy ("Privacy Policy") located at: https://www.cloudberrylab.com/company/privacy-policy.aspx as may be amended from time to time, and incorporated herein by this reference, Company shall provide access to the Subscription Service to Customer during the term of this Agreement. Customer acknowledges and agrees that Company shall have no responsibility for its inability to use the Subscription Service or access the Subscription Service due to network interruption, communications failure, or server downtime.

2. Limited Rights; Ownership

2.1 Company grants to Customer and Customer accepts from Company, a limited, revocable, non-exclusive, non-transferable right to access and use and permit Authorized Users to access and use the Subscription Service solely for the internal business operations of Customer and its Affiliates during the Term. The Subscription Service shall not be used by Customer or by Authorized Users for, or on behalf of, third parties that are not authorized under this Agreement. Customer shall use its best efforts to ensure that the Authorized Users use the Subscription Service in accordance with the terms and conditions of this Agreement. Customer acknowledges that its right to use the Subscription Service will be web-based only pursuant to the terms of this Agreement and that the Subscription Service will not be installed on any servers owned or controlled by Customer or otherwise provided to Customer without Company's consent.

2.2 Authorized Users: Passwords, Access, and Notification. Customer, through its Administrator, shall authorize access to and assign unique passwords and user names for all employees authorized to access the Subscription Service. Authorized User logins are for designated Authorized Users and cannot be shared or used by more than one Authorized User. Customer will be responsible for the confidentiality and use of Authorized User's passwords and user names. Company will act as though any Electronic Communications it receives under Customer's passwords, user name, and/or account number will have been sent by Customer. Customer shall use commercially reasonable efforts to prevent unauthorized access to or use of the Subscription Service and shall promptly notify Company of any unauthorized access or use of the Subscription Service and any loss or theft or unauthorized use of any Authorized User's password or name and/or Subscription Service account numbers.

2.3 Use of the Subscription Service. Customer is responsible for all activities and Electronic Communications conducted by its Authorized Users and for its Authorized Users' compliance with this Agreement, including the content of all Data. Customer will not: (a) sell, lease, license or sublicense the Subscription Service, except as explicitly provided for in this agreement; (b) introduce into or transmit through the Subscription Service any virus, worm, trap door, back door, and other harmful or malicious code, files, scripts, agents, or programs; (c) transmit or transfer infringing material in the Subscription Service; (d) send any Electronic Communication from the Subscription Service that is unlawful, harassing, libelous, defamatory or threatening. Except as permitted by this Agreement, no part of the Subscription Service may be copied, republished, displayed in any form or by any means. Customer agrees not to access the Subscription Service by any means other than through the interfaces that are provided by Company.

Customer represents, covenants, and warrants that Customer will use the Services only in compliance with Company's standard published policies then in effect (the "Policy") and all applicable laws and regulations. Company has no obligation to monitor Customer's use of the Services, Company may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of the foregoing.

Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, "Equipment"). Customer shall also be responsible for maintaining the security of the Equipment, Customer account, passwords (including but not limited to administrative and user passwords) and files, and for all uses of Customer account or the Equipment with or without Customer's knowledge or consent.

Company shall have the right collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, information concerning Customer Data and data derived therefrom), and Company will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Company offerings, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business.] No rights or licenses are granted except as expressly set forth herein.

2.4 Third Party Integrated Services.
Company may allow third party vendors, service providers, software developers and information systems companies to provide applications, websites and/or features via the Company Subscription Service Platform ("integrated Service" or "Integrated Services"). Company may offer Integrated Services by either i) licensing technology from a third party and embedding it in the Subscription Service; or ii) establishing a connection or conduit with a third party's software platform or information system enabling the Subscription Service to send Customer Data or any type of information to the intended party. (i) and (ii) are collectively the "Embedded Technology").

Customer consents to use the Embedded Technology with the Subscription Service. In order to use and subscribe to Embedded Technology, Customer may be required to agree to additional terms and conditions specific to that Embedded Technology.
Integrated Services. Customer acknowledges that: (i) in order to use certain Integrated Services, there may be additionally applicable terms and conditions including those which may establish a direct contractual relationship between Customer and an Integrated Services provider; and (ii); Uptime (as defined in the SLA), availability and support of Integrated Services are excluded from the SLA but may be provided by an Integrated Services provider. If subscribed for Integrated Services, Customer agrees to allow the provider of such Integrated Services to access the Customer's Data as required for the interoperation of that Integrated Service with the Company Subscription Service platform. Customer acknowledges Company is not responsible for any disclosure, modification or deletion of Customer's Data resulting from access by an Integrated Service or its provider. Company does not warrant or support Integrated Services, whether or not they are designated as "certified" or otherwise, unless agreed upon by both parties in writing and incorporated into this agreement as an addendum related to the Integrated Service.

Embedded Technology will be used among other ways to collect data and information ("third party information") from various systems: (i) to identify opportunities in the third party information to be utilized by Customer while using the Subscription Service; (ii) to make improvements to the software underlying the Subscription Service; and (iii) to measure Key Performance Indicators (KPIs). Company has no duty to verify the accuracy or reliability of all such third party information and KPIs and shall not be liable for any loss, damage or expense whatsoever and howsoever arising from any breach or error, loss, damage, or claim caused by Customer or any third party's reliance on any such third party information and KPIs.

2.5 Hosting Center Facilities. The hosting center facilities supporting the Subscription Service, all related Applications and the Third Party Integrated Services where applicable and delivered by Company for usage by the Customer shall be provided for and managed by a third party vendor ("third party vendor") not a party to this Agreement. Company shall not be liable in respect of any breach or error in delivery, loss, damage or interruption to the Subscription Service, Applications or Third Party Integrated Services during the Term of this Agreement caused by the third party vendor. Customer shall immediately notify Company, in writing of any such error, loss, breach, damage or interruption. Company shall not be liable for any loss, damage or expense whatsoever and howsoever arising from any breach or error, loss, damage, defect or interruption to the Subscription Service caused by the third party vendor.

2.6 Security. Each party will use commercially reasonable measures to maintain and enforce physical and logical security procedures to prevent unauthorized access to and/or use of the Subscription Service and the Customer Data. Company will use commercially reasonable measures to secure and defend the Subscription Service against "hackers" and others who may seek to modify or access the Subscription Service or the Customer Data without authorization. Company will use commercially reasonable efforts to remedy any breach of security or unauthorized access. Company shall not be responsible or liable for the disclosure of or unauthorized access to Customer Data caused by Customer, its Authorized Users, Customer's affiliates, or the employees, agents or contractors of any of the foregoing.

2.7 Transmission of Data. The Subscription Service allows Customer to send and receive Electronic Communications and Customer understands that the technical processing and transmission of Customer's Electronic Communications is fundamentally necessary to use of the Subscription Service. Customer acknowledges and understands that Customer's Electronic Communications will involve transmission over the Internet, and over various networks, only part of which may be owned and/or operated by Company. Company is not responsible for any Electronic Communications and/or Customer Data which are delayed, lost, altered, intercepted or stored during the transmission of any data across networks not owned and/or operated by Company, including but not limited to, the Internet and Customer's local network.

2.8 SERVICES AND SUPPORT

Subject to the terms of this Agreement, Company will use commercially reasonable efforts to provide Customer the Services [in accordance with the Service Level Terms attached hereto as Exhibit A]. As part of the registration process, Customer will identify an administrative user name and password for Customer's Company account. Company reserves the right to refuse registration of, or cancel passwords it deems inappropriate.

2.9 Subject to the terms hereof, Company will provide Customer with reasonable technical support services in accordance with the terms set forth in Exhibit B.

2.10 Compliance with Laws. Company will comply with all applicable laws and regulations affecting the operation of Company's business, including any applicable export restrictions and data protection laws. Customer will be solely responsible: (i) for compliance by Customer with all laws and governmental regulations affecting Customer's business, (ii) for using the Subscription Services in a manner to assist it in complying with same, and (iii) the content and accuracy of all reports and documents prepared in whole or in part by using the Subscription Services. Customer will review any calculations made by using the Subscription Services and satisfy itself that those calculations are correct. The Subscription Service is not a substitute for the advice of an attorney and does not include any legal, regulatory, accounting or tax advice and Customer and its affiliates will rely solely upon their own advisors with respect to any such advice. Customer agrees and acknowledges that Company is not a law firm, does not provide legal advice or representation, and that no attorney-client relationship exists or will be formed between Company and Customer.

3. Confidentiality

3.1 Confidential Information. For purposes of this Agreement, "Confidential Information" shall include the terms of this Agreement, Customer Data, each party's proprietary technology, software, code, business processes and technical product information, designs, issues, all communication between the Parties regarding the Subscription Service and any information that is clearly identified in writing at the time of disclosure as confidential. Notwithstanding the foregoing, Confidential Information shall not include information which: (1) is known publicly; (2) is generally known in the industry before disclosure; (3) has become known publicly, without fault of the Receiving Party; (4) the Receiving Party becomes aware of from a third party not bound by non-disclosure obligations to the Disclosing Party and with the lawful right to disclose such information to the Receiving Party; (5) is independently developed by the Receiving Party without use of or reference to the Confidential Information, or (6) is aggregated, de-identified data that does not contain any personally identifiable or Customer-specific information. Each party (the “Receiving Party”) understands that the other party (the “Disclosing Party”) has disclosed or may disclose business, technical or financial information relating to the Disclosing Party’s business (hereinafter referred to as “Proprietary Information” of the Disclosing Party). Proprietary Information of Company includes non-public information regarding features, functionality and performance of the Service. Proprietary Information of Customer includes non-public data provided by Customer to Company to enable the provision of the Services (“Customer Data”). The Receiving Party agrees: (i) to take reasonable precautions to protect such Proprietary Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information after five (5) years following the disclosure thereof or any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party or (e) is required to be disclosed by law.

3.2 Non-Disclosure Obligations. Each party agrees: (a) not to use or disclose Confidential Information except to the extent reasonably necessary to perform its obligations or exercise rights under this Agreement or as directed by the disclosing party; (b) to protect the confidentiality of Confidential Information in the same manner as it protects the confidentiality of similar information and data of its own (at all times exercising at least a reasonable degree of care in the protection of such Confidential Information), and (c) to make Confidential Information available to authorized persons only on a “need to know” basis. Either party may disclose Confidential Information on a need to know basis to its contractors and service providers who have executed written agreements requiring them to maintain such information in strict confidence and use it only to facilitate the performance of their services in connection with the performance of this Agreement. Notwithstanding the foregoing, this Section will not prohibit the disclosure of Confidential Information to the extent that such disclosure is required by law or order of a court or other governmental authority or a regulation.

4. Ownership

4.1 Ownership of Subscription Service. Customer agrees that all rights, title and interest in and to all intellectual property rights in the Subscription Service including without limitation the software used to provide the Subscription Service) are retained and owned exclusively by Company or its licensors. In addition, Company shall have a royalty-free, worldwide, transferable, sub-licensable, irrevocable, and perpetual license to use or incorporate into the Subscription Service and its other product and service offerings any suggestions, enhancement requests, recommendations or other feedback provided by Customer, including Authorized Users, relating to the operation of the Subscription Service and associated services. Any rights not expressly granted herein are reserved by Company. Company service marks and trademarks, logos and product and service names are marks of Company (the "Company Marks"). Customer agrees not to display or use the Company Marks in any manner without Company’s express prior written permission. The trademarks, logos and service marks of Third Party Application providers ("Marks") are the property of such third parties. Customer is not permitted to use these Marks without the prior written consent of such third party who may own the Mark. Except the right to use the Subscription Service, as expressly provided herein, this Agreement does not grant to Customer any rights to, or in, patents, copyrights, Personal Database rights, trade secrets, trade names, trademarks (whether registered or unregistered) or any other rights or licenses with respect to the Subscription Service or the software (the “Software”) used to provide the Subscription Service. Customer will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Subscription Service or any software, documentation or data related to the (“Software”); modify, or create derivative works based on the Subscription Service or any Software (except to the extent expressly permitted by Company or authorized within the Subscription Service). With respect to any Software that is distributed or provided to Customer for use on Customer’s premises or devices, Company hereby grants Customer a non-exclusive, non-transferable, non-sub licensable license to use such Software during the Term only in connection with the Services. The provisions of this paragraph 4.1 shall survive termination of this Agreement.

5.1 Ownership of Customer Data. The information or Customer Data collected by Customer’s use of the Subscription Service shall remain the sole and exclusive property of the Customer unless Company is requested by a government agency or authority, subpoena or court order to produce the Customer Data. Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness of and copyright permissions for all Customer Data. Company will not use the Customer Data for any purpose other than to provide the Services to Customer and to improve the Subscription Service.

5.2 Limited License to Data. Subject to the terms and conditions of this Agreement, Customer grants Company the limited, non-exclusive, non-transferable terminable license to transfer the Data contained in Backup Storage, but only to the extent reasonably necessary to provide the Subscription Service to Customer and to improve the Subscription Service.

6. Payment Terms

6.1 Fees. Customer will pay Company the then applicable fees for the Services and Implementation Services in accordance with the terms therein (the "Fees"). Company reserves the right to change the Fees at the end of the Initial Service Term or then-current renewal term, upon thirty (30) days prior notice to Customer. If Customer believes that Company has billed Customer incorrectly, Customer must contact Company no later than 30 days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Company's customer support department. Company may choose to bill Customer through an invoice, in which case, full payment for invoices issued in any given month must be received by Company no more than thirty (30) days after the mailing date of the invoice. Unpaid amounts are subject to a finance charge of 5% per month on any outstanding balance, or the maximum permitted by law, whichever is lower, plus all expenses of collection and may result in immediate termination of Service.

6.2 Taxes. All Fees payable under this agreement are net amounts and do not include taxes or duties of any kind. Customer will be responsible for, and will promptly pay, any applicable duties, sales tax, use tax, and value added taxes (VAT) or other similar taxes, if any, associated with this Agreement or Customer's receipt or use of the Subscription Service, excluding taxes based on Company's gross or net income or franchise taxes. In the event that Company is required to collect or pay any tax for which Customer is responsible, Customer will pay such tax directly to Company. If Customer is a tax-exempt organization and is not obligated to pay taxes arising out of this Agreement, Customer will provide Company with any required documentation to verify its tax-exempt status with the applicable taxing authorities.

7. Warranties

7.1 *EXCEPT AS STATED IN THE ATTACHED SERVICE LEVEL AGREEMENT, THE SUBSCRIPTION SERVICE IS PROVIDED "AS IS" AND THE COMPANY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. COMPANY DOES NOT REPRESENT THAT CUSTOMER'S USE OF THE SUBSCRIPTION SERVICE, EMBEDDED TECHNOLOGY OR INTEGRATED SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT THE SUBSCRIPTION SERVICE, EMBEDDED TECHNOLOGY OR INTEGRATED SERVICES WILL MEET ALL OF CUSTOMER'S REQUIREMENTS. THE SUBSCRIPTION SERVICE MAY BE TEMPORARILY UNAVAILABLE FOR SCHEDULED MAINTENANCE FOR UNSCHEDULED EMERGENCY MAINTENANCE EITHER BY COMPANY OR THIRD PARTY PROVIDERS, OR BECAUSE OF OTHER CAUSES BEYOND COMPANY'S REASONABLE CONTROL BUT COMPANY SHALL USE REASONABLE EFFORTS TO PROVIDE ADVANCE NOTICE IN WRITING OR BY E-MAIL OF ANY SCHEDULED MAINTENANCE INTERRUPTION.*

TO THE EXTENT PERMITTED BY LAW THE EXCLUSION OR LIMITATION OF CERTAIN WARRANTIES, OR SOME OR ALL OF THE EXCLUSIONS AND LIMITATIONS IN THIS SECTION MAY NOT APPLY TO YOU.

8. Limitations of Liability.

8.1 CUSTOMER ASSUMES THE ENTIRE COST OF ANY DAMAGES RESULTING FROM CUSTOMER'S USE OF THE SUBSCRIPTION SERVICE, EMBEDDED TECHNOLOGY OR INTEGRATED SERVICES (THE "SERVICES"), THE INFORMATION CONTAINED IN OR COMPILED IN THE SERVICES, THE INTERACTION (OR FAILURE TO INTERACT PROPERLY) WITH ANY OTHER HARDWARE OR SOFTWARE WHETHER PROVIDED BY *COMPANY* OR A THIRD PARTY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. IN NO EVENT WILL THE *COMPANY* OR ITS SUPPLIERS BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, SPECIAL, DIRECT, EXEMPLARY, INDIRECT, RELIANCE, INCIDENTAL OR PUNITIVE DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, REVENUE OR SAVINGS, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITIES, LOSS OR CORRUPTION OF BUSINESS INFORMATION OR ANY PERSONAL OR CUSTOMER DATA, LOSS OF GOODWILL, WORK STOPPAGE, HARDWARE OR SOFTWARE DISRUPTION, IMPAIRMENT OR FAILURE, REPAIR COSTS, TIME VALUE OR OTHER PECUNIARY LOSS, OR LOSS OF LIFE) ARISING OUT OF OR RELATING TO THIS AGREEMENT, INCLUDING WITHOUT LIMITATION THE USE

OR INABILITY TO USE THE SERVICES, OR THE INCOMPATIBILITY OF THE SERVICES WITH ANY HARDWARE, SOFTWARE OR USAGE, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH DAMAGES ARE SOUGHT, AND EVEN IF THE COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS. TO THE EXTENT PERMITTED BY LAW THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES, OR SOME OR ALL OF THE EXCLUSIONS AND LIMITATIONS IN THIS SECTION MAY NOT APPLY TO YOU. IF ANY EXCLUSION, DISCLAIMER OR OTHER PROVISION CONTAINED IN THIS AGREEMENT IS HELD TO BE INVALID FOR ANY REASON BY A COURT OF COMPETENT JURISDICTION OR ARBITRATOR AND THE COMPANY BECOMES LIABLE THEREBY FOR LOSS OR DAMAGE THAT COULD OTHERWISE BE LIMITED THE COMPANY'S TOTAL LIABILITY TO YOU OR ANY THIRD PARTIES IN ANY CIRCUMSTANCE IS LIMITED TO THE TOTAL AMOUNT PAID IN SUBSCRIPTION FEES TO THE COMPANY UNDER THIS AGREEMENT FOR THE THREE MONTHS PRIOR TO A CLAIM OF DAMAGES BEING BROUGHT BY CUSTOMER WHETHER IN CONTRACT, TORT OR OTHERWISE.

9. Indemnification

9.1 Company's Indemnity. Company shall, at its own expense, defend Customer from and against any and all allegations, threats, claims, suits, and proceedings brought by third parties (collectively "Claims") alleging that the Subscription Service, as used in accordance with the terms and conditions of this Agreement, infringes the copyrights, trade secrets, patents or trademarks of such third party and shall hold Customer harmless from and against liability, damages, and costs finally awarded or entered into in settlement (including, without limitation, reasonable attorneys' fees) (collectively, "**Losses**") to the extent based upon such a Claim. Excluded from these indemnification obligations are Claims to the extent arising from: (a) use of the Subscription Service in violation of this Agreement or applicable law, (b) use of the Subscription Service after Company notifies Customer to discontinue use because of an infringement claim, (c) modifications to the Subscription Service not made by Company, or (d) use of the Subscription Service in combination with any software, application or service not provided by Company. If a Claim is brought or threatened, Company shall, at its sole option and expense, use commercially reasonable efforts either: (a) to procure for Customer the right to continue using the Subscription Service without cost to Customer; (b) to modify or replace all or portions of the Subscription Service as needed to avoid infringement, such update or replacement having substantially similar or better capabilities; or (c) if the remedies described in (a) and (b) above are not commercially feasible, terminate the Agreement and provide to the Customer any pro-rata refund of the Subscription Service subscription fees pre-paid under the Agreement for the remaining terminated portion of the Term. The rights and remedies granted to Customer under this Section 9.1 state Company's entire liability, and Customer's exclusive remedy, with respect to any claim of infringement of the intellectual property rights of any third party.

9.2 Customer's Indemnity. Customer shall, at its own expense, defend and hold harmless Company from and against any and all Claims, Damages, Losses or Lawsuits alleging: (i) the Customer Data, Customer Content or any Customer trademarks or service marks, or any use thereof, infringes the intellectual property rights or other rights, or has caused harm to a third party; (ii) Customer's or Authorized User's use and misuse of the Subscription Service and failure to comply with all of the Company's policies and Documentation; and (iii) Customer's failure to pay all applicable taxes associated with Customer's use of the Subscription Service. Customer shall defend and hold Company harmless from and against liability for any Losses to the extent based upon such Claims.

9.3 Indemnification Procedures and Survival. In the event of a potential indemnity obligation under this Section 9, the indemnified party shall: (i) promptly notify the indemnifying party in writing of such Claim; (ii) allow the indemnifying party to have sole control of its defense and settlement; and (iii) upon request of the indemnifying party, cooperate in all reasonable respects, at the indemnifying party's expense, with the indemnifying party in the investigation and defense of such Claim. The indemnification obligations under this Section 9 are expressly conditioned upon the indemnified party's compliance with this Section 9.3.

10. Term and Termination.

10.1 Subject to earlier termination as provided below, this Agreement is for the Initial Billing Service Term, and shall be automatically renewed for additional periods of the same duration as the Initial Billing Service Term (collectively, the "Term"), unless either party requests termination at least thirty (30) days prior to the end of the then current billing term.

10.2 In addition to any other remedies it may have, either party may also terminate this Agreement upon thirty (30) days' notice (or without notice in the case of nonpayment), if the other party materially breaches any of the terms or conditions of this Agreement. Customer will pay in full for the Services up to and including the last day on which the Services are provided. [Upon any termination, Company will make all Customer Data available to Customer for electronic retrieval in an agreed upon format for a period of thirty (30) days, but thereafter Company may, but is not obligated to, delete stored Customer Data unless required by law.] All sections of this Agreement which by their nature should survive termination will survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

10.3 Survival. Sections 3, 4, 7, 8, 9 and 12 and any other provisions necessary to interpret the respective rights and obligations of the parties hereunder will survive any termination or expiration of this Agreement, regardless of the cause of such termination or expiration.

Further, Customer may not remove or export from the United States or allow the export or re-export of the Services, Software or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority. As defined in FAR section 2.101, the Software and documentation are "commercial items" and according to DFAR section 252.227-7014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFAR section 227.7202 and FAR section 12.212, any use modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

11. General Provisions.

11.1 Notices. Notices between the parties will be by personal delivery, courier, facsimile transmission, email, or certified or registered mail, return receipt requested, and will be deemed given upon receipt at the address of the recipient party or ten (10) days after deposit in the mail. Addresses used will be the ones set forth above or such other address as a party hereto will notify the other in writing.

11.2 Severability. In the event of any invalidity of any provision of this Agreement, the parties agree that such invalidity will not affect the validity of the remaining portions of this Agreement, and further agree to substitute for the invalid provision a mutually agreeable valid provision that most closely approximates the intent of the invalid provision.

11.3 Headings. The headings in this Agreement are for convenience of reference only and have no legal effect.

11.4 No Third Party Beneficiaries. This Agreement is intended for the sole and exclusive benefit of the signatories and is not intended to benefit any third party. Only the parties to this Agreement may enforce it.

11.5 Assignment. Customer shall not be permitted to assign any of its rights under this Agreement to any other entity (except the right to receive money) without the written consent of Company. Company shall be permitted to assign its rights under this Agreement to any successor entity of any kind.

11.6 Relationship. Each party hereto is an independent contractor, and neither party is, nor will claim to be, a legal representative, partner, franchisee, agent or employee of the other.

11.7 Publicity. Company will not make other use of Customer's name, logo or trademarks or issue any public announcements or press releases regarding this Agreement without Customer's prior written consent.

11.8 Force Majeure. Neither party will be liable to the other for a failure or delay in its performance of any of its obligations under this Agreement (except for the payment of amounts due hereunder) to the extent that such failure or delay is caused by circumstances beyond its reasonable control or by events such as fire, riot, flood, labor disputes, natural disaster, regulatory action, internet or telecommunications failures, terrorist acts, or other causes beyond such party's reasonable control, provided that the non-performing party gives notice of such condition and continues or resumes its performance of such affected obligation to the maximum extent and as soon as reasonably possible.

11.9 Counterparts and Electronic Signatures. This Agreement may be executed in counterparts. A signature transmitted via facsimile, scanned original or third party e-signature system will be deemed an enforceable signature for the purpose of demonstrating the signing party's assent to the Agreement.

11.10 Entire Agreement. This Agreement (including the Exhibits hereto) constitutes the entire understanding and agreement between the parties with respect to the subject matter addressed herein and supersedes any and all prior or contemporaneous oral or written communications with respect to such subject matter. In the event of a conflict between the foregoing terms and conditions and any Exhibits to this Agreement, the foregoing terms and conditions will control. The parties agree that in the event Customer utilizes a purchase order, any term therein which purports to modify or supplement the terms of this Agreement will be void with no force or effect. No modification, termination or waiver of any provisions of this Agreement shall be binding upon a Party unless in writing signed by an authorized officer of the relevant Party(ies).

12 Governing Law

12.1 Governing Law/Arbitration. By using the Services, you agree that the laws of the State of California, without regard to principles of conflict of laws, will govern this Agreement and any dispute of any sort that might arise between you and the Company.

12.2 Disputes

ANY DISPUTE RELATING IN ANY WAY TO YOUR USE OF THE SUBSCRIPTION SERVICE SHALL BE SUBMITTED TO CONFIDENTIAL BINDING ARBITRATION IN ORANGE COUNTY, CALIFORNIA EXCEPT FOR INTELLECTUAL PROPERTY CLAIMS BROUGHT BY EITHER PARTY (WHICH FOR PURPOSES OF THIS SECTION DO NOT INCLUDE PRIVACY AND PUBLICITY CLAIMS) AND CLAIMS THAT MAY BE BROUGHT IN SMALL-CLAIMS COURT.

CONFIDENTIAL ARBITRATION UNDER THIS AGREEMENT SHALL BE RESOLVED EXCLUSIVELY UNDER THE CONSUMER ARBITRATION RULES THEN PREVAILING OF THE AMERICAN ARBITRATION ASSOCIATION ("AAA'S CONSUMER RULES"), EXCLUDING ANY RULES AND PROCEDURES GOVERNING OR PERMITTING CLASS OR REPRESENTATIVE ACTIONS. THE RULES ARE AVAILABLE AT THE AMERICAN ARBITRATION ASSOCIATION'S WEBSITE.

YOU AND COMPANY AGREE TO EXPRESSLY WAIVE ANY RIGHTS TO FILE CLASS OR REPRESENTATIVE ACTIONS OR SEEK RELIEF ON A CLASS OR REPRESENTATIVE BASIS IN ANY JURISDICTION OR FORUM.

THE ARBITRATOR SHALL APPLY CALIFORNIA LAW, AND THE ARBITRATOR'S AWARD SHALL BE BINDING AND MAY BE ENTERED AS A JUDGMENT IN ANY COURT OF COMPETENT JURISDICTION. THERE SHALL BE NO APPEAL FROM ANY AWARD OF THE ARBITRATOR. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, NO ARBITRATION UNDER THIS AGREEMENT SHALL BE JOINED TO AN ARBITRATION INVOLVING ANY OTHER PARTY SUBJECT TO THIS AGREEMENT, WHETHER THROUGH CLASS ARBITRATION PROCEEDINGS OR OTHERWISE. IF ANY PART OF THIS ARBITRATION PROVISION IS FOUND TO BE INVALID, UNENFORCEABLE OR ILLEGAL, THE REST OF THIS PROVISION SHALL REMAIN IN EFFECT.

IF THE ENTIRE ARBITRATION PROVISION IS FOUND TO BE INVALID OR UNENFORCEABLE, THEN THE PARTIES CONSENT TO PERSONAL JURISDICTION AND EXCLUSIVE VENUE IN THE STATE AND FEDERAL COURTS IN ORANGE COUNTY, CALIFORNIA.

EXHIBIT A
Service Level Agreement

The Company agrees to provide the Customer the Service for any computers the Customer has licensed using the CSPs of the Customer's choice and / or any storage under the control of Customer. The Company will use all reasonable commercial efforts to make sure that the Service is available 24 hours per day, 7 days a week, as subject to the conditions of this Service Level Agreement ("SLA"), further described below.

Service Level Conditions:

- Backups are based upon the configuration schedules Customer has selected. However, certain issues with Customer's computers, internet connectivity, network, or other technical issues outside the Company's control may cause a scheduled backup to not complete or fail to run. It is the Customer's sole responsibility to ensure that a backup has completed. The Company is not responsible for failed backups.
- Restore of backup files is at the Customer's discretion. Restore times are not guaranteed and may depend on many factors, including, but not limited to, internet bandwidth, network bandwidth, computer resources, and size of backup files to be restored.
- Some CSPs may provide a service to send a hard drive with backup data directly to Customer. The Company will not assist Customer with this process.
- The Company may perform scheduled maintenance at times determined at Company's sole discretion. Maintenance will be completed in as short a time as reasonably possible. The Service may be unavailable or operate with reduced performance during such maintenance. This maintenance is necessary to insure the reliability and managed features of the Service. The Company may post notices through the Service letting Customer know when maintenance is planned. However, there may be times when emergency maintenance is required and notification by Company to Customer in these cases may not be possible. When possible, the Company will post a notice through the web site or email indicating when the Service will be restored.
- The Company cannot account for issues affecting the Service outside of Company's control. As such, Company makes no warranties or guarantees with regards to the availability of the Service or Customer's ability to connect to and use the Service.

EXHIBIT B
Support Terms

- All Support services are performed remotely. As such, the Company will not send technicians to Customer's home or place of business to address any issues that you may have.
- The Company offers phone, email, and remote diagnostic support according to the following schedule:
- **Monday through Friday:** 2 am – 8 pm Eastern Time (UTC-05:00)
- **Saturday and Sunday:** 8 am – 2 pm Eastern Time (UTC-05:00)
- **Holidays:** Support times during major international holidays is available the same times as Saturday and Sunday
- The Company offers phone and remote diagnostic support by customer request only. These services should be scheduled by Customer in advance. Customer may initiate a support call by calling +1 212-863-9918 during open support hours or by emailing support@cloudberrylab.com at any time. Company will use commercially reasonable efforts to respond to all support inquiries within one (1) business day.

Cloud Services

MASTER CUSTOMER AGREEMENT

THIS MASTER CUSTOMER AGREEMENT (“Agreement”) is is made by and between Druva and the entity that has licensed from Druva products and services (“Customer”) either directly or through reseller with which Customer contracted.

BY ACCEPTING THIS AGREEMENT, EITHER BY INDICATING ACCEPTANCE, BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, OR BY UTILIZING/ ACCESSING THE DRUVA PRODUCTS AND SERVICES, CUSTOMER AGREES TO THE TERMS OF THIS AGREMEENT. THIS AGREEMENT IS A LEGALLY BINDING CONTRACT BETWEEN CUSTOMER AND DRUVA AND SETS FORTH THE TERMS THAT GOVERN THE LICENSE(S) PROVIDED TO CUSTOMER HEREUNDER.

1. **Definitions**.

(a) **“Affiliate”** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. **“Control”** for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) **“Authorized Users”** means natural persons who are authorized by Customer to use the Cloud Services, as applicable, and who actively use the Cloud Services.

(c) **“Cloud Services”** means Druva’s software-as-a-service solution for managing data availability and information governance, any feature or functionality add-ons, and any modified versions of, and upgrades, updates and additions to such solution, ordered by Customer under an Order Form.

(d) **“Cloud Storage Area”** means the geographic storage area provided by Druva where Customer Data may be stored per Customer’s instructions.

(e) **“Confidential Information”** means all confidential or proprietary information disclosed by a party (“Disclosing Party”) to the other party (“Receiving Party”), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Customer’s Confidential Information excludes Customer Data. Confidential Information will not include information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party without use of or reference to the Disclosing Party’s Confidential Information.

(f) **“Customer Data”** means data, information and materials of Customer or its Authorized Users that Customer or its Authorized Users uploads to, stores on, or accesses with Druva’s Cloud Services.

(g) **“Customer Site”** means the geographic location at which Customer Data may be collected.

(h) **“Documentation”** means the published user guides, manuals, instructions and/or specifications provided or made available to Customer with respect to the Cloud Services.

(i) **“Indemnified Liabilities”** means any (i) settlement amounts approved by the indemnifying party; (ii) damages and costs in a final judgment awarded against the indemnified part(ies) by a competent court; and (iii) all attorneys’ fees, and court or tribunal costs incurred by either party with respect to defense and settlement of such third-party claim.

(j) **“Indirect Tax**” means without limitation, value-added tax, goods and services tax, sales and use and similar transaction taxes, and gross receipts tax, as the case may be.

(k) **“Order Form”** means an order confirmation of Druva (or an Affiliate of Druva) or other written document (e.g., purchase order) that identifies Druva’s products and services ordered by Customer, directly or through the Reseller with which Customer contracted, which is accepted by Druva (or an Affiliate of Druva) in writing, but shall exclude any pre-printed or linked terms and conditions set forth in such written document that are in addition to, inconsistent or in conflict with, or different than, this Agreement. The term “Reseller” in this Agreement shall refer to a reseller or a distributor of Druva’s Cloud Services, as applicable.

(l) **“Taxes”** means taxes, levies, duties or similar national, federal, state, provincial, or local governmental assessments of any nature, including Indirect Tax, that are assessable by any jurisdiction under applicable law.

(m) **“Term”** means the period during which Druva’s products and services, as applicable, are initially contracted to be available to Customer under this Agreement as set forth in the Order Form(s), unless terminated earlier under this Agreement. After the initial term and unless terminated earlier pursuant to this Agreement, this Agreement shall automatically renew for successive 1 year terms, unless either party provides the other party with written notice of termination at least 30 days prior the end of this Agreement’s then-current term. For Phoenix products, “Term” shall commence on the effective date and continue thereafter until the earliest of (i)

Customer runs out of pre-purchased credits and provides Druva with 30 days' advance written notice of termination or (ii) the Agreement is terminated by either party pursuant to Section 12(c).

(n) **"Third-Party Legal Proceeding"** means any formal legal proceeding filed by an unaffiliated third party before a court.

2. Cloud Services License.

Subject to Customer's compliance with this Agreement, Druva hereby grants Customer a non-transferable, non-exclusive, revocable, limited, and restricted license to access and use the Cloud Services for Customer's own internal business purposes only in a manner pursuant to this Agreement and the applicable Documentation for the Term unless earlier terminated. For Customers purchasing inSync or Phoenix or both, Druva shall use commercially reasonable efforts to make the Cloud Services available to Customer in accordance the service levels attached hereto as Exhibit A during the Term unless earlier terminated. Customer may install and use the Cloud Services on any of Customer's compatible endpoint devices up to the maximum number of permitted Authorized Users and storage limit per Authorized User set forth in the Order Form. Customer may make copies of the Documentation for its own internal use in connection with its use of the Cloud Services in accordance with this Agreement, but no more than the amount reasonably necessary.

3. Privacy and Confidentiality.

(a) **Privacy**. Customer authorizes Druva to transmit, backup and use Customer Data solely to provide the Cloud Services to Customer and Customer's Affiliates. For Customers subject to General Data Protection Regulation, Druva agrees to comply with its data processor obligations under the Data Processing Addendum. For additional information on Druva's privacy practices, please visit our Privacy Policy.

(b) **Confidentiality**. The Receiving Party agrees to use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind, but not less than reasonable care. Each party shall not (i) disclose the other party's Confidential Information to any third parties other than as expressly provided in this Agreement, (ii) use the other party's Confidential Information for purposes outside the scope of this Agreement, and (iii) disclose the other party's Confidential Information, unless to directors, employees, or consultants who have a need to know such information and are subject to confidentiality obligations that are at least as restrictive as those contained in this Agreement.

(c) **Data Storage**. The Cloud Services will process and store Customer Data in the Cloud Storage Area selected by Customer, except as necessary to comply with the law or a valid binding order of a law enforcement agency. In the event that Druva has the capability and desires to change the location of the Cloud Storage Area for a Customer Site, Druva agrees to promptly notify Customer in writing and provide all relevant details of the desired change to the location of the Cloud Storage Area, and not change the location of the Cloud Storage Area without Customer's prior written approval, which Customer may withhold in its sole discretion.

(d) **Usage and Configuration Metrics**. Druva, its Affiliates, and its third-party service providers that perform services in connection with Druva's performance of this Agreement may collect information regarding number of users, number of devices, number of servers, per user storage capacity, aggregate storage usage and storage locations of the Customer (which information shall not include any Customer Data, or any "personal identifiable information" or "protected health information" as such terms are defined in applicable U.S. privacy laws) . Druva, its Affiliates, and its third-party service providers may use such information only for their internal business purposes, including to perform and to ensure compliance with this Agreement. Druva, its Affiliates, and its third-party service providers agree to keep such information confidential.

4. Customer Information.

(a) **Ownership**. As between Druva and Customer, Customer retains title to and ownership of all right, title, and interest in the Customer Data.

(b) **Customer Responsibility**. Customer is solely responsible for (i) maintaining the confidentiality of its Authorized Users' credentials, passwords, and encryption keys associated with its accounts, (ii) properly configuring the settings of the Cloud Services and taking its own steps to maintain appropriate security and protection of passwords and encryption keys and settings for any backup of Customer Data, (iii) all activities that occur with respect to Customer's accounts regardless of whether the activities are undertaken by it, its employees, or a third party (including its contractors or agents), (iv) its and its Authorized Users' access and use of the Cloud Services and compliance with this Agreement and the applicable Documentation (v) all content of Customer Data, and (vi) all product settings, which may override individual end point settings of Authorized Users, if applicable. Druva is not responsible for any alteration, compromise, corruption, or loss of Customer Data that arises from any access to, sharing, or use of Customer's accounts, credentials, passwords, or encryption keys.

5. Ownership.

Any authorized copies that Customer makes, the Cloud Services, and the Documentation are the intellectual property of and are owned by Druva and its Affiliates and their licensors, and constitute the confidential information of Druva. As between Druva and Customer, Druva and its Affiliates retain title to and ownership of all right, title and interest in the Cloud Services and the Documentation, including all intellectual property and other proprietary rights therein, and subject to the applicable limited licenses expressly granted by Druva to Customer in Section 2. Customer does not have any right, title, or interest in the Cloud Services or the Documentation. To the extent that the Cloud Services contain or may be provided with components that are offered under an open source license, Druva agrees to make that license available to Customer and the provisions of that license may expressly override some of the terms set forth in this Agreement for such components. All rights not expressly granted in this Agreement are reserved by Druva and its Affiliates and their licensors.

6. **Restrictions and Requirements**.
   (a) **Proprietary Notices.** Customer and its Authorized Users will not remove or modify any trademarks, trade names, service marks, service names, logos or brands, or copyright or other proprietary notices on the Cloud Services or the Documentation, or add any other markings or notices to the Cloud Services or the Documentation.
   (b) **Use Obligations.** Customer and its Authorized Users (i) will access and use the Cloud Services in accordance with this Agreement and the applicable Documentation, (ii) will not use or permit the Cloud Services to perform any file storage or other services for any third party, (iii) will not use or permit the Cloud Services to upload any Customer Data that (A) infringes the intellectual property rights or other proprietary rights of any third party, (B) is unlawful or objectionable material, or (C) contains software viruses or other harmful or deleterious computer code, files, or programs, such as trojan horses, worms, time bombs, or cancelbots, (iv) will not use or permit the use of any software, hardware, application, or process that (A) interferes with the Cloud Services, (B) interferes with or disrupts servers, systems, or networks connected to the Cloud Services, or violates the regulations, policies, or procedures of such servers, systems. or networks, (C) accesses or attempts to access another customer's accounts, servers, systems, or networks without authorization, (D) harasses or interferes with another customer's use and enjoyment of the Cloud Services, or (E) in Druva's sole discretion, inordinately burdens the resources of Druva or its Affiliates that are providing the Cloud Services, or (v) will not tamper with or breach the security of the Cloud Services.
   (c) **Prohibited Activities**. Customer and its Authorized Users will not (i) modify, port, adapt, translate or create any derivative work based upon the Cloud Services or the Documentation, (ii) reverse engineer, decompile, disassemble, or otherwise derive or attempt to derive the source code of the Cloud Services, except for any non-waivable right to decompile the Cloud Services expressly permitted by applicable mandatory law, (iii) copy, distribute, sell, assign, pledge, sublicense, lease, loan, rent, timeshare, use or offer the Cloud Services on a service bureau basis, deliver or otherwise transfer the Cloud Services, in whole or in part (iv) access Cloud Services to create competitive products to Druva or engage in the competitive analysis of Cloud Services .

7. **Payment Terms**.
   (a) **Fees**. Customer shall pay Druva, directly or through the Reseller with which Customer contracted, the subscription fees, overages (if applicable) and other amounts for Druva's products and services ordered by Customer, in United States currency (unless otherwise specified in the Order Form) (collectively, the "Fees"). For Phoenix Products, Subscription Fees apply to pre-paid Phoenix credits Customer has contracted for. Overages will be calculated and invoiced monthly and will subject to on-demand pricing, which will be an incremental 10% increase to the Supscription Fees. All payment obligations are non-cancellable, and all Fees paid to Druva are non-refundable except as expressly set forth in this Agreement.
   (b) **Payment Terms**. All Fees will be invoiced in advance in accordance with the Order Form. Unless otherwise set forth in the Order Form, all Fees are due and payable Net 30 days after the date of the applicable invoice. All invoices that are not paid within Net 30 days, and all credit accounts that are delinquent, shall be assessed a 1.5% late payment charge (or, if less, the highest legal rate under applicable law) for each month the invoice is not paid or the account is delinquent. Customer will reimburse Druva for all reasonable costs (including reasonable attorneys' fees) incurred by Druva in connection with collecting any overdue amounts.
   (c) **Taxes**. With respect to the transactions and payments contemplated in this Agreement, each party shall be solely responsible to pay all Taxes and governmental fees and charges (and, any penalties, interest, and other additions thereto) that each party is liable to pay under applicable law or otherwise under this Agreement. All Fees payable under this Agreement are exclusive of applicable Taxes. If either party has an obligation under applicable law or this Agreement to pay or collect Indirect Tax for which the other party is legally liable or responsible under this section, then the paying or collecting party will invoice the other party for such Indirect Tax, which the invoiced party will pay. The invoice will satisfy requirements under applicable law for a valid tax invoice. Each party will provide the other party with such information as is reasonably required to determine whether there is an obligation to pay or collect Indirect Tax. Neither party shall pay or collect any Indirect Tax from or on behalf of the other party for which, under applicable law, (i) the other party has previously provided to the paying or collecting party a properly completed and valid exemption certificate, or (ii) the parties may otherwise claim an available, valid exemption from such Indirect Tax.

8. **Limited Warranty**.
   (a) **Authority.** Each party represents and warrants that (i) this Agreement has been duly entered into and constitutes a valid and binding agreement enforceable against such party in accordance with its terms; (ii) no authorization or approval from any third party is required in connection with such party's entering into or performance of this Agreement; and (iii) the entering into and performance of this Agreement does not violate the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound.
   (b) **Limited Warranty**. Druva warrants that Cloud Services will perform substantially in accordance with the applicable published specifications when used in accordance with this Agreement and the Documentation for the Term of the Agreement. Non-substantial variations of performance from the published specifications or other Documentation do not establish a warranty right. This limited warranty is void if failure of the Cloud Services has resulted from installation, deployment, use, maintenance or support not in accordance with the Documentation, modification by Customer, an Authorized User or a third party not authorized by Druva, force

majeure, or any breach of this Agreement by Customer or an Authorized User. In the event of a Cloud Services warranty claim, Customer's sole and exclusive remedy and Druva's entire obligation and liability shall be, at Druva's sole option, to either (i) provide a correction, update or upgrade of the Cloud Services, (ii) correct or replace the Cloud Services, or (iii) refund Customer, directly or through the Reseller with which Customer contracted, a pro-rated amount of the applicable Fees pre-paid by Customer covering the whole months that would have remained, absent such early termination, in the Term following the effective date of such early termination and terminate this Agreement. Any corrected, upgraded or updated version of the Cloud Services will be warranted for the remainder of the warranty period. All warranty claims must be made to Druva in writing within such warranty period.

(c) **General Disclaimer**. EXCEPT AS EXPRESSLY SET FORTH IN SECTIONS 8(a) AND 8(b), THE CLOUD SERVICES ARE PROVIDED "AS IS" AND (i) DRUVA SPECIFICALLY DISCLAIMS ANY AND ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (ii) DRUVA DOES NOT WARRANT THAT THE CLOUD SERVICES OR ANY PART THEREOF, OR USE THEREOF WILL BE UNINTERRUPTED, ERROR-FREE, UNBREACHABLE OR VIRUS FREE, OR WILL MEET CUSTOMER'S QUALITY AND PERFORMANCE REQUIREMENTS. CUSTOMER ASSUMES THE ENTIRE RISK OF AND SHALL NOT HOLD DRUVA RESPONSIBLE FOR ANY ALTERATION, COMPROMISE, CORRUPTION OR LOSS OF CUSTOMER DATA, NOTWITHSTANDING ANY SECURITY OR OTHER MEASURE THAT MAY BE PROVIDED BY DRUVA.

9. Indemnification.

(a) **Customer.** Customer, if notified promptly in writing and given authority, control, information and assistance at Customer's expense for defense and settlement of same, shall defend and indemnify Druva and Druva's Affiliates, employees, officers, directors, agents, successors, and assigns against any Indemnified Liabilities, in any Third Party Legal Proceeding so far as it relates to the content of Customer Data, including intellectual property infringement right claims.

(b) **Druva.** Subject to Sections 9(b) (Exceptions), Druva, if notified promptly in writing and given authority, control, information and assistance at Druva's expense for defense and settlement of same, shall defend and indemnify Customer against Indemnified Liabilities, in any Third Party Legal Proceeding so far as it is based on a claim that the use of the Cloud Services furnished under this Agreement infringes a United States patent that has been issued as of the installation or deployment date, as the case may be. If Druva reasonably believes that Customer's use of the Cloud Services is likely to be enjoined, or if the Cloud Services are held to infringe such patent and all use of such Cloud Services by Customer is thereby enjoined, Druva shall, at its expense and at its sole option, (i) procure for Customer the right to continue using the Cloud Services, (ii) replace the Cloud Services with other non-infringing software or services of substantially equivalent functionality, or (iii) modify the Cloud Services so that there is no infringement, provided that such modified software or services provide substantially equivalent functionality. If, in Druva's opinion, the remedies in clauses (i), (ii) and (iii) above are infeasible or commercially impracticable, Druva may, in its sole discretion, refund Customer, directly or through the Reseller with which Customer contracted, a pro-rated amount of the applicable Fees pre-paid by Customer covering the whole months that would have remained, absent such early termination, in the Term following the effective date of such early termination and terminate this Agreement. Customer shall not settle any matter without the prior written approval of Druva.

(c) **Exceptions**. The indemnification obligation in this Section 9 will not apply to the extent the infringement is caused by any of the following: (i) the Cloud Services is modified in an unauthorized manner by Customer, (ii) the Cloud Services is combined with other unauthorized software, hardware, application or process by Customer, (iii) the Cloud Services is used in violation of this Agreement or the Documentation by Customer, (iv) any third party deliverables or components contained within the Cloud Services that are not provided by Druva, or (v) any materials, data or information provided by Customer, including Customer Data.

(d) **Sole Remedy**. THIS SECTION 9 SETS FORTH CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND DRUVA'S ENTIRE OBLIGATION AND LIABILITY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

10. Limitation of Liability.

EXCEPT FOR EITHER PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 9 AND CUSTOMER'S MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, PUNITIVE, SPECIAL, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY TYPE OR KIND (INCLUDING LOSS OF BUSINESS, GOODWILL, REVENUE, USE OR OTHER ECONOMIC ADVANTAGE, BUSINESS INTERRUPTION, OR ANY ALTERATION, COMPROMISE, CORRUPTION OR LOSS OF CUSTOMER DATA) ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THE CLOUD SERVICES, THE DOCUMENTATION OR USE THEREOF OR THIS AGREEMENT, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT FOR THE EXCLUSIONS SET FORTH IN THE PRECEDING SENTENCE, EACH PARTY'S AGGREGATE LIABILITY UNDER THIS AGREEMENT SHALL BE LIMITED TO THE FEES PAID AND PAYABLE BY CUSTOMER FOR THE CLOUD SERVICES FOR THE TWELVE MONTHS IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO THE CLAIM. FOR CLARITY, THE ABOVE LIMITATIONS SHALL NOT LIMIT CUSTOMER'S PAYMENT OBLIGATIONS UNDER SECTION 7. No claim against Druva may be brought more than one year after the facts giving rise to such claim have arisen. The limitations of liability and exclusions of damages in this Section 10 form an essential basis of the bargain between the parties and shall survive and apply even if any remedy specified in this Agreement is found to have failed its essential purpose.

11. **Insurance**.

Druva shall maintain, at its expense, during the Term workers' compensation insurance as required by applicable law, and commercial general liability insurance, errors and omissions liability insurance, cyber security insurance, and umbrella liability insurance from financially sound insurance companies having coverages and limits of liability that are commercially reasonable. Upon request, Druva will provide Customer with proof of such insurance.

12. **Suspension; Termination.**

(a) **Suspension.** In the event of any actual or threatened breach of this Agreement by Customer (including non-payment of fees), without limiting Druva's other rights and remedies and notwithstanding anything in this Agreement to the contrary, Druva may immediately suspend Customer's use of the Cloud Services.

(b) **Termination.** This Agreement may only be terminated by a party upon written notice to the other party (i) if the other party breaches a material term of this Agreement that is uncured within 30 days (or, in the case of non-payment, 15 days) after delivery of notice of such breach, or (ii) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors not dismissed within 30 days. In the event the cost of providing Cloud Services exceeds the Fees paid and payable by Customer, Druva will notify Customer and Customer shall work with Druva in good faith to remediate the issue. If no resolution is found within 60 days from the date of the notice to Customer, then Druva may either terminate the Agreement or increase the Fees. Notwithstanding the above, Druva may immediately terminate this Agreement without prior written notice or an opportunity to cure in the event of an actual or threatened breach of Section 2, 5, or 6.

(c) **Fees**. Upon expiration of this Agreement, Customer will pay Druva, directly or through the Reseller with which Customer contracted, any unpaid amounts that are owed to Druva for the Term. Upon termination of this Agreement based on Customer's breach (following any applicable cure period), Customer will pay Druva any unpaid amounts that would have been owed to Druva for the remainder of the then-current Term if such early termination had not occurred as well as any other amounts owed to Druva under this Agreement, without limiting Druva's other rights and remedies. Upon termination of this Agreement based on Druva's breach (following any applicable cure period), Druva will refund Customer, directly or through the Reseller with which Customer contracted, any amounts pre-paid under this Agreement for the remaining full calendar months in the then-current Term.

(d) **Effect (inSync).** Upon expiration or termination of this Agreement, the license rights granted by Druva to Customer under this Agreement will cease immediately and Customer will immediately cease all use of the Cloud Services, as applicable, and delete (or, at Druva's request, return) related Documentation, passwords and any Druva confidential information in its possession or control. Upon expiration or termination of this Agreement (other than termination by Druva for breach), at the Customer's written request made within 30 days after expiration, Druva will provide Customer with temporary access to the Cloud Services solely for Customer to retrieve its back-up of the Customer Data (but not for any other purpose) and/or provide, at its standard export fee, a copy of its Customer Data on a portable storage device. If applicable, and after such 30-day period, Druva will have no obligation to maintain or provide access to the Customer Data and will thereafter, unless legally prohibited, delete all Customer Data stored on the Cloud Services.

Effect (Phoenix). Upon termination of this Agreement, the license rights granted by Druva to Customer under this Agreement will cease immediately and Customer will immediately cease all use of the Cloud Services, as applicable, and delete (or, at Druva's request, return) related Documentation, passwords and any Druva confidential information in its possession or control. If at the time of termination Customer has outstanding Phoenix credits, Customer will have 60 days following the termination of this Agreement to use up the remaining credits and then 30 days to retrieve its back-up of the Customer Data and/or Druva will provide, at its standard export fee, a copy of the Customer Data on a portable storage device. After such 90-day period Druva will have no obligation to maintain or provide access to the Customer Data and will thereafter, unless legally prohibited, delete all Customer Data stored on the Cloud Services. If at the time of termination Customer has no outstanding Phoenix credits, Customer will have 30 days following the termination of this Agreement to retrieve its then-current back-up of the Customer Data and/or Druva will provide, at its standard export fee, a copy of the Customer Data on a portable storage device. After such 30-day period Druva will have no obligation to maintain or provide access to the Customer Data and will thereafter, unless legally prohibited, delete all Customer Data stored on the Cloud Services.

Effect (CloudRanger). Upon expiration or termination of this Agreement, the license rights granted by Druva to Customer under this Agreement will cease immediately and Customer will immediately cease all use of the Cloud Services, as applicable, and delete (or, at Druva's request, return) related Documentation, passwords and any Druva confidential information in its possession or control. Druva shall delete any account data no later than 30 days after the expiration or termination of the Agreement, unless legally prohibited.

(e) **Survival.** Sections 4, 5, 6, 7, 8, 9, 10, 12 and 13 will survive the expiration or termination of this Agreement.

13. **General.**

(a) **Parties**. Druva and Customer are independent contractors. Nothing in this Agreement shall be deemed to constitute a joint venture or partnership between the parties, nor constitute any party as the agent of the other party for any purpose or entitle any party to commit or bind the other party in any manner. Nothing in this Agreement, express or implied, (nor if this Agreement is governed by Singapore law, under the Contracts (Rights of Third Parties) Act, Chapter 53B of Singapore) is intended to confer upon any party other than the parties hereto, Druva's Affiliates and their licensors and their respective successors and permitted assigns any rights or obligations.

(b) **Governing Law, Jurisdiction and Attorneys' Fees**. Pursuant to the table below, Druva contracting entity and the applicable law will depend on where Customer is domiciled.

If Customer is domiciled in:	**Customer is contracting with:**	**The governing law is:**	**The courts having exclusive jurisdiction are:**
A country in North America or South America	Druva, Inc. a Delaware corporation	California and controlling United States federal law	Santa Clara, California, U.S.A.
A country in Asia Pacific	Druva Technologies Pte. Ltd., a Republic of Singapore company	Singapore law	Singapore
Japan		Japan law	Tokyo, Japan
A country in India subcontinent (which includes India, Pakistan, Sri Lanka, Bangladesh, Nepal and Bhutan)	Druva Data Solutions Private Limited	India law	Mumbai, India
A country in Europe, Middle East, or Africa	Druva Europe Limited, an England and Wales, United Kingdom company	Wales and England law	London, England
Germany		German law	Frankfurt, Germany

Unless California laws apply, THE PARTIES HEREBY WAIVE ANY RIGHTS THEY MAY HAVE TO TRIAL BY JURY. This Agreement shall not be governed by the conflict of law rules of any jurisdiction, the United Nations Convention on Contracts for the International Sale of Goods or the Uniform Computer Information Transactions Act, the application of which is expressly excluded. If any action is pursued to enforce this Agreement, the prevailing party shall be entitled to reasonable attorneys' fees and costs, in addition to any other relief to which such party may be entitled.

(c) **Export Laws**. Customer understands that the Cloud Services and the export and re-export of data via the Cloud Services may be controlled by the laws of one or more countries governing technology use and transfer, including U.S. Export Administration Regulations. Customer will not use or transfer any technology or data in violation of such laws.

(d) **Publicity**. Customer authorizes Druva to use Customer's name, logo, and/or trademark in connection with marketing, sales, financial, public relation, and other materials used for promotional and marketing activities only.

(e) **Entire Agreement; Amendment; Waiver**. This Agreement, together with the Exhibit and the Order Form(s), is the parties' entire agreement with respect to its subject matter, and supersedes any prior communications, discussions, understandings or agreements. Any term of this Agreement may be amended and the observance of any term of this Agreement may be waived with the written consent of duly authorized representatives of the parties.

(f) **Severability**. If any provision of this Agreement is held to be unenforceable, the unenforceable provision shall be replaced by an enforceable provision that comes closest to the parties' intentions underlying the unenforceable provision, and the remaining provisions of this Agreement shall remain in full force and effect. The unenforceability of any provision in any jurisdiction shall not affect the enforceability of such provision in any other jurisdiction.

(g) **Subcontracts; Assignment**. Druva may subcontract any services to be performed under this Agreement without Customer's consent and without providing notice. Druva may assign or transfer this Agreement, in whole or in part, to any Affiliate or in connection with any acquisition, consolidation, merger, reorganization, transfer of all or substantially all of its assets or other business combination, or by operation of law without Customer's consent and without providing notice. Customer may not assign or transfer any part of this Agreement by business combination, operation of law or otherwise without Druva's prior written consent. Subject to the foregoing, this Agreement will bind and benefit the parties and their respective successors and permitted assigns.

(h) **Data Center Providers.** Customer hereby consents to data center providers supply hosting services for the Cloud Services. For the purposes of this Agreement, such data center providers will not be considered subcontractors.

(i) **Force Majeure.** Druva shall not be liable for its inadequate performance caused by any condition beyond the reasonable control of Druva or its suppliers, including accidents, acts of God or nature, government acts, civil unrest, acts of war or terrorism, third-party criminal acts, strikes or other labor problems, failures in computer, hardware, telecommunications, internet service provider or hosting facilities, power shortages, and denial of service attacks.

(j) **Notices.** All notices given under this Agreement shall be in writing and shall be deemed given upon receipt. All notices shall be sent to the parties at their respective address on the Order Form, or to such email address or address as subsequently modified by written notice given in accordance with this section.

(k) **Counterparts**. This Agreement may be signed in counterparts, including via facsimile, pdf or other electronic reproduction, and any such counterpart will be valid and effective for all purposes.

Exhibit A

inSync and Phoenix: Service Level Agreement (SLA) for Cloud Services

Cloud Services Availability

The Cloud Services will be available 24 hours per day, 7 days per week, excluding any scheduled maintenance as described below.

Category 1 – Scheduled Maintenance.

InSync: A weekly scheduled maintenance period may be scheduled every Saturday between **10 AM** UTC to **1 PM** UTC to perform system maintenance, backup, and upgrade functions for the Cloud Services. If scheduled maintenance is required outside of the weekly scheduled maintenance period described above, Druva will notify Customer at least three business (3) days in advance.

Phoenix: A weekly scheduled maintenance period may be scheduled on the first and third Monday of each month at **5am** UTC (Phoenix Cloud) and at **8am** UTC (Phoenix GovCloud) for a maximum duration of 90 minutes to perform system maintenance, backup, and upgrade functions for the Cloud Services. If scheduled maintenance is required outside of the weekly scheduled maintenance period described above, Druva will notify Customer at least three business (3) days in advance.

Category 2 – Unscheduled Maintenance. Unscheduled maintenance may be required to resolve issues that are critical for Customer and/or performance of the Cloud Services. Druva will use its commercially reasonable efforts to notify Customer via email at least six (6) hours prior to the unscheduled maintenance.

Durability of Customer Data

Druva shall ensure 99.99999% Customer Data durability.

Uptime and Service Credits

Please reference the following table (Reporting Period = Calendar Month), which details the credit available to Customer in the event Cloud Services Availability falls below the indicated thresholds:

InSync

Cloud Services Availability	Credits
< 99.5% in one Reporting Period	5% of one (1) month of Fees
< 99% in one Reporting Period	10% of one (1) month of Fees

Phoenix

Cloud Services Availability	Credits
< 99.5% in one Reporting Period	5% of one (1) Phoenix Month*
< 99% in one Reporting Period	10% of one (1) Phoenix Month

Additionally, if the Cloud Services Availability falls below 95% for three (3) consecutive Reporting Periods, Customer shall have the right to terminate this Agreement and such right must be exercised within ten (10) days of the end of such three (3) month period or Customer shall be deemed to have waived its termination right with respect to that particular three (3) month period.

* Phoenix month is equivalent to the value of the Phoenix credits consumed by Customer for the affected month.

Calculation of Cloud Services Availability

Cloud Services Availability = (Total Hours in Reporting Period – Unscheduled Maintenance which causes unavailability – Scheduled Maintenance) / (Total Hours in Reporting Period – Scheduled Maintenance) X 100%.

*Excluded means the following: (i) unavailability caused by force majeure; (ii) any problems resulting from Customer combining or merging the Cloud Services with any hardware or software not supplied by Druva or not identified by Druva in writing as compatible with the Cloud Services; (iii) interruptions or delays in providing the Cloud Services resulting from telecommunications or Internet service provider failures; or (iv) any interruption or unavailability resulting from Customer's use of the Cloud Services in an unauthorized or unlawful manner or any interruption resulting from the misuse, improper use, alteration or damage of the Cloud Services.

Request for Credit for Cloud Services Availability

Any Customer request for a credit that Customer is entitled to under this SLA may only be made on a calendar month basis and must be submitted within ten (10) days after the end of the relevant calendar month or shall be deemed to have been waived by Customer.

For those periods at the end of a Term that do not coincide with the end of a calendar month, Customer must make a claim for a credit within ten (10) days after the expiration of the Term or the claim for credit shall be deemed to have been waived by Customer.

The right to a credit and/or the right to terminate this Agreement under this SLA and this Agreement shall be the sole and exclusive remedy available to Customer in the event of unavailability of the Cloud Services and, under no circumstance, shall the unavailability of the Cloud Services be deemed a breach by Druva of its obligations under this Agreement.

End User License Agreement

IMPORTANT: THIS AGREEMENT IS PROOF OF YOUR RIGHT TO USE DRUVA'S SOFTWARE AND CONTAINS ADDITIONAL INFORMATION CONCERNING PRODUCT WARRANTY AND LIMITATIONS OF LIABILITY. PLEASE READ IT CAREFULLY.

This End-User License Agreement ("EULA") is a legal agreement between you and the business entity you represent (collectively "CUSTOMER") and Druva Software Private Limited (hereinafter "DRUVA"). Druva is willing to grant you the following rights.

DRUVA IS WILLING TO GRANT YOU THE FOLLOWING RIGHTS TO USE THE SOFTWARE ONLY IF YOU AGREE TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN DRUVA IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM DRUVA OR AN AUTHORIZED DRUVA RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

1. DEFINITIONS:The software incorporated in or supplied and accompanying documentation, shall collectively termed "Druva Software". The term "Licensed Software" is understood to specially include any and all Licensed Software and Documentation but specifically does not include open-source components. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the Software and made available by Druva with the Software in any manner (including on CD-Rom, printed, or on-line). "Permitted Number" means one (1) unless otherwise indicated under a valid license (e.g. volume license) granted by Druva. "Computer" means an electronic device that accepts information in digital or similar form and manipulates it for a specific result based on a sequence of instructions. "License keys" shall mean activation codes provided directly by Druva or its partners that are used by licensed users of the Druva Software to activate its functionality for an authorized Computer. An authorized Computer is identified by a signature build of hardware parts unique serial numbers or alternatively, a USB dongle.

2. OWNERSHIP:The Druva Software is and shall remain a proprietary product of Druva. Druva shall retain ownership of all patents, copyrights, trademarks, trade names, trade secrets and other proprietary rights relating to or residing in the Druva Software. Except for the license grant provided in Section 3, you shall have no right, title or interest in or to the Druva Software. The Druva Software is licensed, not sold, to you for use only under the terms of this Agreement. All rights not specifically granted in this EULA are reserved by Druva.

3. GRANT OF LICENSE:Druva grants you a non-transferable (except as set forth in this Section) non-exclusive, restricted right to use the Druva Software solely in connection with the operation of the Equipment for your own internal business purposes. You may install and use a copy of the Software on your compatible computer, up to the Permitted Number of computers. You understand that Druva may update the Druva Software at any time and in doing so incurs no obligation to furnish such updates to you pursuant to this Agreement.

4. RESTRICTIONS:Druva reserves all rights in the Druva Software not expressly granted to you. Except as permitted in Section 3, you may not use, copy, modify, create derivative works of, distribute, sell, assign, pledge, sublicense, lease, loan, rent, timeshare, deliver or otherwise transfer the Druva Software, nor permit any other party to do any of the foregoing. You may not remove from the Druva Software, or alter, any of the trademarks, trade names, logos, patent or copyright notices or markings, or add any other notices or markings to the Druva Software. To the extent permissible by applicable law, you may not derive or attempt to derive the source code of the Druva Software by any means, nor permit any other party to derive or attempt to derive such source code. To the extent permissible by applicable law, you may not reverse engineer, decompile, disassemble, or translate the Druva Software or any part thereof.

5. LIMITED WARRANTY:Druva warrants to the person or entity that first purchases a license for the Software for use pursuant to the terms of this license, that the Software will perform substantially in accordance with the Documentation for the ninety (90) day period following receipt of the Software when used on the recommended hardware configuration. Non-substantial variations of performance from the Documentation does not establish a warranty right. THIS LIMITED WARRANTY DOES NOT APPLY TO UPDATES, PRE-RELEASE, TRYOUT, PRODUCT SAMPLER, OR BETA SOFTWARE. To make a warranty claim, you must return the Software to the location where you obtained it along with proof of purchase within such ninety (90) day period. Druva does not warrant that the functions contained in the Druva Software will meet your requirements or that the operation of your Druva Software will be uninterrupted or error free. This limited warranty is void if failure of the Druva Software to conform with the warranty, has resulted from improper installation, testing, misuse, neglect, accident, fire or other hazard, or any breach of this Agreement.

6. LIMITED REMEDIES:In the event of a breach of the foregoing limited warranty, you must return the Druva Software to Druva or the Druva authorized reseller that provided you with the Druva Software, postage prepaid, before the expiration of the warranty period, with a copy of the invoice for the unit. Druva’s sole and exclusive obligation and your sole and exclusive remedy shall be, at Druva’s sole discretion, to either * Provide a replacement copy of the Druva Software or * Refund the amount you paid for the Druva Software and terminate this Agreement. Any replacement copy of the DRUVA Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

7. NO OTHER WARRANTIES:OTHER THAN THE FOREGOING LIMITED WARRANTY, DRUVA HEREBY EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE AND MERCHANTABILITY.

8. LIMITATION OF LIABILITY: DRUVA'S AGGREGATE LIABILITY IN CONNECTION WITH THIS AGREEMENT, REGARDLESS OF THE FORM OF THE ACTION GIVING RISE TO SUCH LIABILITY (WHETHER IN CONTRACT, TORT OR OTHERWISE), SHALL NOT EXCEED THE AMOUNT PAID BY YOU DIRECTLY TO DRUVA OR PAID BY YOU TO DRUVA THROUGH AN AUTHORIZED RESELLER. DRUVA SHALL NOT BE LIABLE TO YOU FOR ANY INDIRECT, EXEMPLARY, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES OF ANY KIND (INCLUDING WITHOUT LIMITATION LOSS OF DATA, EQUIPMENT DOWNTIME OR LOST PROFITS), EVEN IF DRUVA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. THE LIMITED WARRANTY, LIMITED REMEDIES AND LIMITED LIABILITY PROVISIONS CONTAINED IN THIS AGREEMENT ARE FUNDAMENTAL PARTS OF THE BASIS OF DRUVA'S BARGAIN HEREUNDER, AND DRUVA WOULD NOT BE ABLE TO PROVIDE THE DRUVA SOFTWARE TO YOU ABSENT SUCH LIMITATIONS.

9. Open Source Software Components : The License Software is shipped in the same medium as open source software components that are specifically not covered by this Agreement. This EULA only covers software components that have been developed and are propriety of Druva. The Open Source software components aggregated in the same medium as Licensed Software have their own end user license agreements.

10. GENERAL TERMS:

10.1 The Warranty and the End User License shall be governed by the laws of the State of California, USA, without regard to conflicts of laws principles. You hereby consent to the exclusive jurisdiction of the state and federal courts in Santa Clara County, California, USA to resolve any disputes arising under this Agreement.

10.2 No Druva reseller, agent or employee is authorized to make any amendment to this Agreement. Druva and other trademarks contained in the Software are trademarks or registered trademarks of Druva Software Private Limited. Third party trademarks, trade names, product names and logos may be the trademarks or registered trademarks of their respective owners. You may not remove or alter any trademark, trade names, product names, logo, copyright or other proprietary notices, legends, symbols or labels in the Software.

To learn more about Druva,

druva

Druva Support Policies

Copyright Notice

Any technical documentation that is made available by Druva Inc. (“Druva”) is the copyrighted work of Druva and is owned by Druva. Druva reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Druva.

Trademarks

Windows® is a U.S. registered trademark of Microsoft Corporation. Linux is a U.S. registered trademark of Linus Torvalds. Red Hat® Enterprise Linux® is a registered trademark of Red Hat Inc. Ubuntu is a registered trademark of Canonical Ltd. Apple, Mac and Mac OS are trademarks of Apple Inc. Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Disclaimer

The information contained in this document is subject to change without notice. Druva Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the performance, or use of this manual.

This document outlines policy and guidelines adopted by the Druva Support team to ensure smooth customer experience. This document contains proprietary, confidential, and legally privileged information for the sole use of the person or entity to which this document is originally addressed. Any review, e-transmission dissemination or other use of or taking of any action in reliance upon this information by persons or entities other than the intended recipient is strictly prohibited.

Table of Contents

Revision history

Revision	Date	Changes
1.0	April 2012	First edition
2.0	May 2015	Added information about EOL policies
2.1	September 2015	Added details about improved case submissions, new Support Portal, and Premium Support Policy

Overview

At Druva, we are committed to provide timely support services to our customers. We provide support services to assist our customers with technical queries, licensing information, and issues regarding the Druva products. Our services are available 24x7x365, and English is the primary language of support.

For assistance, you can either browse through our online resources or create a support case through Druva Support Portal.

Druva Support Service Offerings

Druva Support offers Business Critical and Premium Support.

Each issue is unique and carries a different set of complexities and challenges. Druva Support will make all reasonable efforts to provide a response within the assigned time frame.

The following table gives a brief comparison between Business Critical and Premium Support services.

Support Type	Business Critical		Premium Support (Offered Separately)	
Priority	**Initial**	**Follow Up**	**Initial**	**Follow Up**
Critical	1 Hour	4 Hours	30 mins.	2 Hours
High	2 Hours	8 Hours	1 Hour	4 Hours
Medium	4 hours	24 Hours	2 Hours	12 Hours
Low	8 Hours	48 Hours	4 Hours	24 Hours

Click here to know more about the Business Critical Support.

Click here to know more about Premium Support.

Priority levels

You or the Druva support engineer can specify the priority of the service request. The following table provides guidelines about the priority definitions:

Priority	Description
Critical	The Druva product is unavailable which critically affects your production environment. You observe a complete loss of service. A workaround is not yet available.
High	The Druva product is affected, and your production environment is running but impacted. You observe a severe loss of service. A workaround is not yet available.
Medium	A function in Druva product has failed; however, your production environment is not affected. You observe a minor loss of service. Druva Support is aware of the issue and a workaround is available.
Low	No impact to the functionality of Druva Product and to your production environment or business. This includes requests about the Druva Product, such as an enhancement, information, documentation, and how-to questions. You observe no loss of service.

Support Portal features

Druva Support Portal provides time-saving tools to solve problems, answer questions, share documentation, and create a case. Druva provides the following online support services.

Knowledge

Search for solutions and technical documents that contain information about common problems and steps to resolve the issues. Notifications about releases are also available on Knowledge.

Forums

Druva Forums is your community hub where you can post questions to the community, exchange information, and connect with your technical peers. With each interaction, you can also earn reward points.

Create and track a case

Create, update, manage, and track your case online. For more information, see Case Submission.

Announcements

Druva posts Product announcements, release notes, and alerts on a regular basis. Click here, to read the latest announcements.

How to get Support?

General Information

You can contact Druva Technical Support in the following ways:

- Support Portal

- Chat
- Telephone

Support Portal

By logging in to the Druva Support Portal, you can choose to submit a case, initiate a chat, or find the telephone numbers to contact the Druva support engineers. You can also browse the Druva **Knowledge** and **Forums** to engage with the Druva customers, partners, and experts.

Chat Support

Chat support allows you to directly contact Druva technical support. To deliver best experience and right person for the issue, Druva requires you to log into the support portal and click Chat Now. You will be presented with the following options:

1. Select a Case
2. Select case type

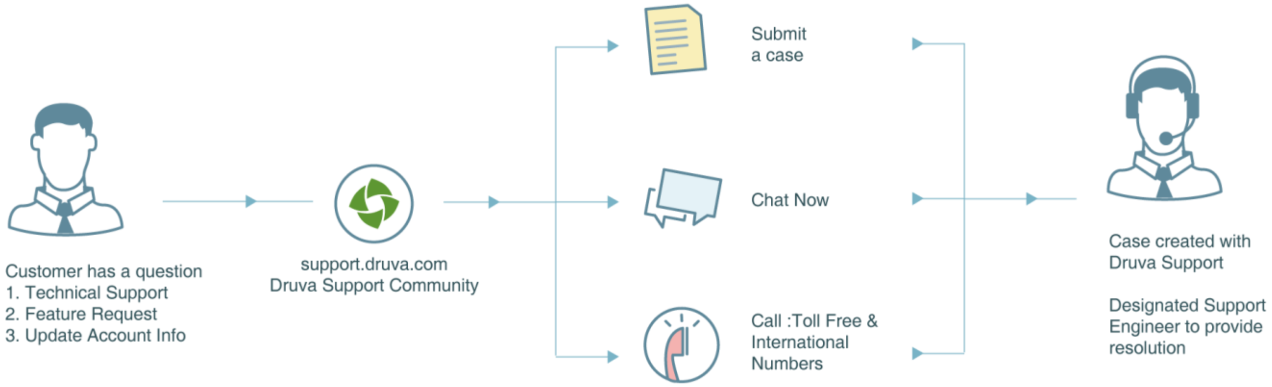
Based on your support requirement, you can select an existing case or open a new case by selecting the case type to initiate chat with Druva technical support.

Telephone Support

The Druva technical support is available 24x7x365 to answer your questions. For information about Druva technical support phone numbers, see the **Contact Us** section on https://support.druva.com. All customers are entitled to receive telephone support 24x7x365.

Case submission

The following illustration depicts the different ways to contact Druva Support and submit a case:



How to submit a case?

1. Open https://support.druva.com and login to the Druva Support Portal. If you are a new user, click here to register on the Druva Support Portal.
2. Click the **Submit a Case** option under the **Support Quick Links** section.
3. On the **Submit a New Case** page, provide the following information.

   - Issue description, priority, and case type.
   - Product details, such as product and its version, operating system details.
   - Attachments that include screen captures of the issue, log files, and relevant information.

   The information that you provide helps the Support team to work on your case quickly and effectively.

4. Click **Submit a Case**.

When you enter the case details, related articles will be displayed to help you resolve your issue. If the suggested articles do not provide the information that you require, you can proceed to submit the case.

You can track the status of your case and add your comments online. You can even change the priority of the case or escalate the case.

Note: For critical issues that affect your business and need immediate action, Druva recommends that you create a case and then call Druva Support. Please ensure that you have the case number handy when you call Druva Support. For information about Druva Support phone numbers, see the **Contact Us** section on https://support.druva.com.

Information to be provided during case submission

While resolving your case, the support engineer will request you to provide key information or to perform certain tasks. Following are the tasks that you might have to perform:

- Provide clear description and system information while reporting an issue.
- Provide specific logs from the system and perform tests to generate debug logs.
- Involve networking, database, or other technology-specific administrators to help troubleshoot the issue.
- Involve relevant third-party software vendors or hardware vendors wherever required. For example, operating system vendors and database vendors.

How to escalate a case?

You can escalate your case if you require assistance on a higher priority and quick response from the assigned engineer.

To escalate a case:

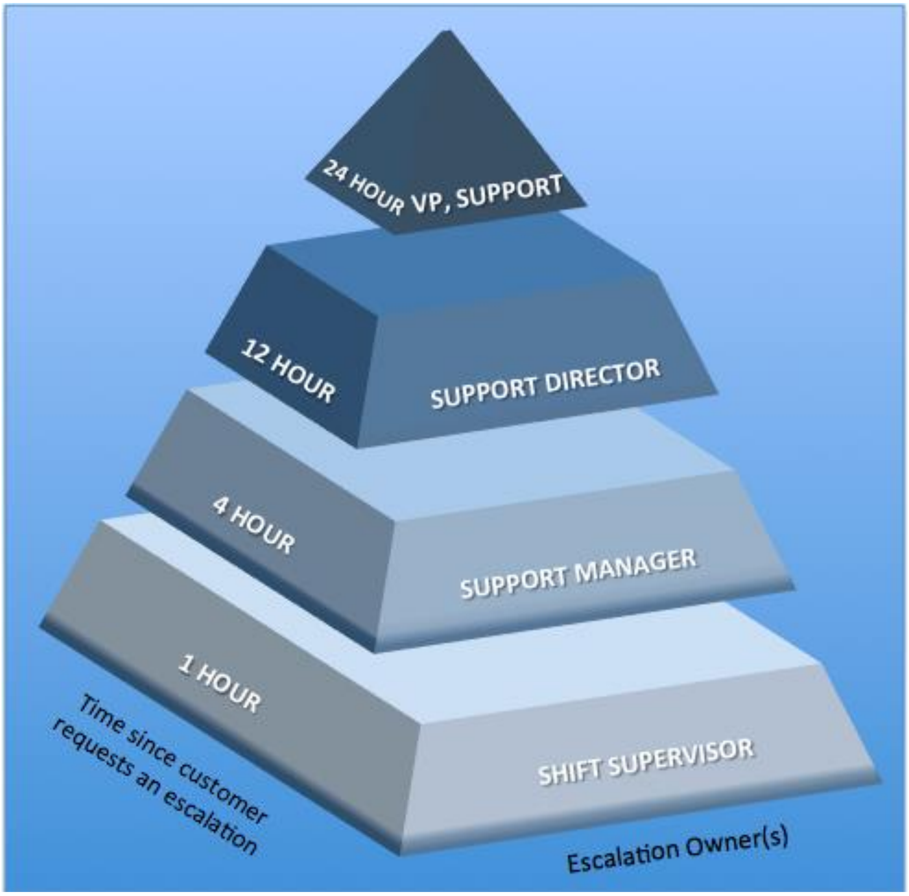
1. Login to the Druva Support Portal.
2. Open the case you want to escalate.
3. Click on the **Request Escalation** link that is available at the bottom of the comments section.

In addition, you can call Druva Support and request to speak to the Team Manager regarding your escalation.

Note: Please ensure that you have the case number handy when you call Druva Support. For information about Druva Support phone numbers, see the **Contact Us** section on https://support.druva.com.

Druva ensures that your case gets the required visibility until the issue is addressed. The following diagram provides information about the escalation process. As per the time required to address the issue, the visibility will automatically change to the next highest level to ensure swift assistance.

Escalation process



Best Practices

Getting started

The Get started quick link on the Druva Support Portal provides the most popular resources and links to our growing Druva end user community and support experts. On the **Getting Started** page, you can do the following:

- Find procedures to install inSync Cloud and inSync On-Premise in 5 easy steps.
- Subscribe to the Cloud Notifications. The **Support Portal Home** page and the **Getting started** page both provide Cloud Notification and Announcements.

Self-Service

- Check whether the issue and workaround is already available at **Forums** and **Knowledge**.
- Browse through our extensive Documentation Portal that provides Release Notes details, feature descriptions, procedures, FAQ's, and troubleshooting tips for the Druva products.
- Inform Druva about any changes in the contacts and support category of your organization in order to keep your profile up-to-date.

Professional Services

Professional services from Druva enable you to get the most out of your inSync deployment while saving IT time and resources. Reduce internal resources required to deploy and manage inSync, benefit from Druva's expertise, and customize your inSync deployment to meet your needs. Refer the following link to know more about Professional services that Druva offers:
https://www.druva.com/professional-services/

Training

Our goal is to enable you to successfully operationalize Druva products in your environment. Our courses are designed with extensive hands on exercises using Druva Training Cloud Lab, which means you get to practice new concepts while they are being introduced in the class. As you successfully complete all lab exercises, you will feel confident about getting your organization off to a great start with Druva.
You can check our available training courses here: www.druva.com/training/

EOL Policies

Druva is not obligated to provide technical support beyond the end-of-life (EOL) period.

EOL Policy for inSync On-Premise

Each release of inSync On-premise comes with new features and enhancements. Druva also releases patches and hotfixes for inSync On-premise as and when required.

As per Druva's EOL policy, Druva discontinues inSync On-premise versions that are more than 2 years old. For all other versions, Druva provides product support for 1 year. If any other version of the product is supported for more than 2 years, Druva informs the customers through the EOL page.

EOL for an inSync On-premise version means an end to all technical assistance, auto-upgrades, and bug fixes for that version. During the release, Druva publishes the tentative EOL date for inSync On-premise. Six months prior to the planned EOL date, Druva starts sending periodic reminders to its customers to ensure that they have sufficient time to upgrade.

To view the supported inSync On-premise versions, see inSync On-premise Support.

EOL Policy for inSync client

Each release of inSync client comes with new features and enhancements. Druva also releases patches and hotfixes for the inSync client as and when required.

As per Druva's end-of-life (EOL) policy, Druva discontinues versions of the inSync client that are more than 15 months old.

EOL for an inSync client version means an end to all technical assistance, auto-upgrades, and bug fixes for that version. During an inSync release, Druva publishes the tentative EOL date for the inSync client. Six months prior to the planned EOL date, Druva starts sending periodic reminders to its customers to ensure that they have sufficient time to upgrade.

Druva recommends that you periodically upgrade inSync clients installed on user laptops to the latest version. To view the supported inSync client versions, see inSync Cloud support and EOL policies.

EOL policy for inSync mobile app

Each release of the inSync mobile app comes with new features and enhancements. Druva also releases patches and hotfixes for the inSync mobile apps as and when required.

Ad per Druva's end-of-life (EOL) policy, Druva supports the last three major versions on iOS and Android mobile devices. Druva also supports Windows Phone 8.x on the Windows Phone platform.

EOL for an inSync mobile app means an end to all technical assistance, auto-upgrades, and bug-fixes for that version. Druva recommends that you periodically upgrade your mobile device OS to the latest version. To view the supported inSync mobile app versions, see inSync Cloud support and EOL policies.

EOL policy for inSync Cloud Cache

Each release of inSync Cloud Cache comes with new features and enhancements. Druva also releases patches and hotfixes for inSync Cloud Cache as and when required.

As per Druva's end-of-life (EOL) policy, Druva supports the last two versions of inSync Cloud Cache.

EOL for an inSync Cloud Cache version means an end to all technical assistance, auto-upgrades, and bug-fixes for that version. Druva recommends that you periodically upgrade inSync Cloud Cache to the latest version.

EOL policy for inSync AD Connector

Each release of inSync AD Connector comes with new features and enhancements. Druva also releases patches and hotfixes for inSync AD Connector as and when required.

As per Druva's end-of-life (EOL) policy, Druva supports the last two versions of inSync AD Connector.

EOL for an inSync AD Connector version means an end to all technical assistance, auto-upgrades, and bug-fixes for that version. Druva recommends that you periodically upgrade the inSync AD Connector to the latest version.

EOL policy for Phoenix Client

Each release of Phoenix client provides new features and enhancements. Druva also releases patches and hotfixes for the Phoenix client as and when required. Druva recommends that you periodically upgrade Phoenix clients to the latest version.

The following policies are applicable to Phoenix:

1. **EOS (end of support)**. Druva ends all support for the Phoenix client versions that are more than 18 months old, and no patches are made available. Auto-upgrades will continue to work. Druva starts sending periodic reminders to its customers to ensure that they upgrade Phoenix clients to the latest version.

2. **EOL (end of life)**. EOL for a Phoenix client version means an end to all technical assistance, auto-upgrades, and bug fixes for that version. Phoenix client versions that are more than 24 months old may stop connecting to the cloud and all backups/restores may be blocked. During a Phoenix release, Druva publishes the tentative EOL date for the Phoenix client. Six months prior to the planned EOL date, Druva starts sending periodic reminders to its customers to ensure that they have sufficient time to upgrade.

EOL Policy for Phoenix Cloud Cache

Each release of Phoenix Cloud Cache provides new features and enhancements. Druva also releases patches and hotfixes for Phoenix Cloud Cache as and when required.

As per Druva's end-of-life (EOL) policy, Druva supports the last two versions of Phoenix Cloud Cache. EOL for an Phoenix Cloud Cache version means an end to all technical assistance, auto-upgrades, and bug-fixes for that version. Druva recommends that you periodically upgrade Phoenix Cloud Cache to the latest version.

Duo Security is now a part of Cisco

Contact Sales

Free Trial

Service Terms and Conditions

EFFECTIVE AS OF MAY 25TH, 2018

These Service Terms and Conditions (“Agreement”) constitute a contract between Duo Security, Inc. with offices at 123 North Ashley Street, Suite #200, Ann Arbor, MI 48104 (“Duo Security”), and you. Duo Security wishes to provide and you wish to have the right to access pursuant to the terms of this Agreement, a subscription service. This Agreement includes and incorporates the webpage Order Form with which you purchased the Services and any subsequent Order Forms (submitted in written or electronic form). By accessing or using the Services, you agree to be bound by this Agreement. If you are entering into this Agreement on behalf of a company, organization or other entity, you represent that you have such authority to bind such entity and are agreeing to this Agreement on behalf of such entity. If you do not have such authority to enter into this Agreement or do not agree with these terms and conditions, you may not use the Services.

1. DEFINITIONS

1.1 “Applicable Law” means the Data Protection Laws and any other applicable laws, rules and regulations.

1.2 “Customer” means the customer that has signed up for the Services and agreed to the terms of this Agreement.

1.3 “Customer Data” means any information or data about Customer or Users (and its and their staff, customers or suppliers, as applicable) that is supplied to Duo Security by or on behalf of Customer or any User in connection with the Services, or which Duo Security is required to access, generate, process, store or transmit pursuant to this Agreement, including (without limitation) information about Customer’s and Users’ respective devices, computers and use of the Services. Customer Data shall not be deemed to include any Performance Data.

1.4 “Customer Personal Data” means any Customer Data that is personal data (as defined under the applicable Data Protection Laws).

1.5 “Data Protection Laws” means all data protection and privacy laws, rules and regulations applicable to a party and binding on that party in the performance of its obligations under this Agreement, including, where applicable, EC Directive 2002/58/EC and Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

1.6 “Documentation” means guides, instructions, policies and reference materials provided to Customer by Duo Security in connection with the Services, including the documentation located at https://www.duo.com/docs, which Duo Security may amend from time to time.

1.7 “Duo Admin Panel” means the web portal currently accessible at https://admin.duosecurity.com, which allows Customer’s internally appointed administrator(s) of the Services to, among other options, enroll and activate Users, issue and manage SMS passcodes and bypass codes, and manage mobile devices (as applicable to the Services set forth on the applicable Order Form).

1.8 “Duo Mobile Software” means all Duo Security proprietary mobile applications used in providing the Services, and any updates, fixes or patches developed from time to time.

1.9 “Fees” means the applicable fees as set forth on the Order Form.

1.10 “Free Services” means those aspects of the Services that are free and do not require payment, such as beta features or functionality or, in the case of a free trial, the Services themselves.

1.11 “Hardware Tokens” means hardware security tokens purchased by Customer under an Order Form.

1.12 “Intellectual Property Rights” means all patents, registered designs, unregistered designs, design rights, utility models, semiconductor topography rights, database rights, copyright and other similar statutory rights, trade mark, service mark and any know how relating to algorithms, drawings, tests, reports and procedures, models, manuals, formulae, methods, processes and the like (including applications for any of the preceding rights) or any other intellectual or industrial property rights of whatever nature in each case in any part of the world and whether or not registered or registerable, for the full period and all extensions and renewals where applicable.

1.13 “Order Form(s)” means the invoice or other forms from Duo Security for the initial order for the Service, and any subsequent invoice or other forms from Duo Security (submitted in written form or online), specifying, among other things, the maximum number of Users, initial Term, purchase of any Hardware Tokens, Fees, Telephony Credits (if any), and such other charges and terms as agreed between the parties.

1.14 “Payment Schedule” means the schedule selected by Customer for payment of Fees (on either an order webpage or an attached Order Form), which may be either monthly by credit card or annually or multi-year and invoiced in advance, with payment due within thirty (30) days of receipt of invoice.

1.15 “Performance Data” means any and all aggregate, de-identified data relating to the access or use of the Services by or on behalf of Customer or any User, including any performance, analytics or statistical data, that Duo Security may collect from time to time.

1.16 “Service Level Agreement” or “SLA” means the description of the availability of the Services located at: https://www.duo.com/legal/sla.

1.17 “Services” means the products and services that are ordered by or made available to Customer under a free trial or an Order Form, including, where applicable, the Software, Hardware Tokens and services using only the Duo Mobile Software, and made available online by Duo Security, including associated offline components, as described in the Documentation.

1.18 “Software” means (i) Duo Security proprietary software (including the Duo Mobile Software), and (ii) open source software used by Duo Security in providing the Services which integrates with Customer’s network or application, including SSL or other VPN, Unix operating system, Microsoft application, or web application, as provided in the Documentation and any updates, fixes or patches developed from time to time.

1.19 “Telephony Credits” mean credits for Customer’s Users to provide authentication by telephone or SMS.

1.20 “Term” means the subscription term indicated on the Order Form and any subsequent renewal terms.

1.21 “User” means any user of the Services whom Customer may authorize to enroll to use the Services under the terms of this Agreement.

2. SERVICES FOR CUSTOMER; DUO SECURITY OBLIGATIONS

2.1 Subject to and conditioned on Customer’s payment of Fees and full compliance with all other terms and conditions of this Agreement, Duo Security grants Customer and Users a non-exclusive, non-sublicensable, non-transferable license to access and use the Services, along with such Documentation as Duo Security may make available during the Term. Duo Security Services are provided for commercial use only, not for private use.

2.2 The Services and SLA are subject to modification from time to time at Duo Security’s sole discretion, provided the modifications do not materially diminish the functionality of the Services provided by Duo Security and the Services continue to perform according to the description of the Services specified in Section 2.3 in all material aspects. Customer shall have the right to terminate the Agreement pursuant to Section 10.2 without any penalty if (i) a material modification to the Services or the SLA is made which materially diminishes the functionality of the Services or materially diminishes the SLA, (ii) Duo Security has not obtained Customer’s consent for such modifications and (iii) Duo Security does not provide a remedy in the cure period stated in Section 10.2.

2.3 Duo Security will make the Services available and the Services will perform substantially in accordance with the description of the services found at https://www.duo.com/pricing. Notwithstanding the foregoing, Duo Security reserves the right to suspend Customer’s (or any User’s) access to the Services immediately (i) in the event that Customer breaches Section 4 or Section 7 of this Agreement, or breaches any other provision of this Agreement and fails to correct that breach within the applicable cure period; or (ii) as it deems reasonably necessary to respond to any actual or potential security or availability concern that may affect customers or Users.

2.4 Subject to full compliance with the terms and conditions of this Agreement, in the event that Customer earns 15 days of service credits, determined in accordance with the terms of the Service Level Agreement, in each of three consecutive months, Customer may terminate this Agreement and, as its sole and exclusive remedy, receive a refund of any pre-paid subscription Fees paid by Customer to Duo Security for Services not rendered as of the termination date. The SLA shall not apply with respect to Free Services and Duo Security is not obligated to provide support with respect to any Free Services.

3. CUSTOMER RESPONSIBILITIES

3.1 Customer may only use the Services in accordance with the Documentation and as explicitly set forth in this Agreement. Customer will cooperate with Duo Security in connection with the performance of this Agreement as may be necessary, which may include making available such personnel and information as may be reasonably required to provide the Services or support. Customer is solely responsible for determining whether the Services are sufficient for its purposes, including but not limited to, whether the Services satisfy Customer’s legal and/or regulatory requirements.

3.2 Customer shall not provide any infringing, offensive, fraudulent or illegal content in connection with the Services, and Customer represents and warrants that any content it provides will not violate any Intellectual Property Rights of any third party. Duo Security reserves the right, in its sole discretion, to delete or disable any content submitted by Customer that may be infringing, offensive, fraudulent or illegal. To view Duo Security's complete copyright dispute policy and learn how to report potentially infringing content, please visit: https://duo.com/legal/copyright.

3.3 Use of the Services may require Users to install Duo Mobile Software on their mobile devices, which use shall be subject to this Agreement. Customer's use of third party products or services that are not licensed to Customer directly by Duo Security ("Third Party Services") shall be governed solely by the terms and conditions applicable to such Third Party Services, as agreed to between Customer and the third party. Duo Security does not endorse or support, is not responsible for, and disclaims all liability with respect to Third Party Services, including without limitation, the privacy practices, data security processes or other policies related to Third Party Services. Customer agrees to waive any claim against Duo Security with respect to any Third Party Services.

3.4 Customer acknowledges that the Services will require Users to share with Duo Security certain information which may include personal information regarding Users (such as usernames, Duo Admin Panel passwords, email address and/or phone number) solely for the purposes of providing and improving the Services. Prior to authorizing an individual to become a User, Customer is fully responsible for obtaining the consent of that individual, in accordance with Applicable Law, to the use of his/her information by Duo Security, which use is described in Duo Security's Services Privacy Notice, located at https://duo.com/legal/privacy-notice-services. Customer represents and warrants that all such consents have been or will be obtained prior to authorizing any individual to become a User.

3.5 Customer will be fully responsible for Users' compliance with this Agreement and any breach of this Agreement by a User shall be deemed to be a breach by Customer. Duo Security's relationship is with Customer and not individual Users or third parties using the Services through Customer, and Customer will address all claims raised by its Users, and third parties using the Services through Customer, directly with Duo Security. Customer must ensure that all third parties that utilize the Services through Customer agree (a) to use the Services in full compliance with this Agreement, and (b) to the extent permitted by Applicable Law, to waive any and all claims directly against Duo Security related to the Services.

4. RESTRICTIONS

Customer will not, and will not permit any Users nor any third party to: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of the Services, Software, Hardware Tokens or any data related to the Services (except to the extent such prohibition is contrary to Applicable Law that cannot be excluded by the agreement of the parties); modify, translate, or create derivative works based on the Services or Software; share, rent, lease, loan, resell, sublicense, distribute, use or otherwise transfer the Services or Software for timesharing or service bureau purposes or for any purpose other than its own use, except as expressly provided in an applicable Order Form; or use the Services or Software other than in accordance with this Agreement and in compliance with Applicable Law.

5. PAYMENT OF FEES

5.1 Customer will pay Duo Security the Fees plus all applicable sales, use and other purchase related taxes (or provide Duo Security with a valid certificate of exemption from the requirement of paying sales, use or other purchase related taxes) in accordance with the Payment Schedule and payment terms set forth on the Order Form. Customer shall be responsible for all taxes related to the Services and this Agreement, exclusive of taxes on Duo Security's income. Except as otherwise indicated in the applicable Order Form, all fees and expenses shall be in U.S. dollars. Unpaid and due Fees are subject to a finance charge of one percent (1.0%) per month, or the maximum permitted by law, whichever is lower, plus all expenses of collection, including reasonable attorneys' fees, except to the extent Applicable Law requires a different interest or finance charge calculation for unpaid and due Fees and expenses. In the case of any withholding requirements, Customer will pay any required withholding itself and will not reduce the amount paid to Duo Security on account thereof. If the method of payment is by credit card, Customer agrees to (i) keep Customer's credit card information updated and (ii) authorize charging Customer's credit card the Fees when due. Duo Security will not charge Users any fees for their use of the Services or Duo Mobile Software without Customer's authorization and the Duo Mobile Software can be downloaded by Users free of charge. Users' carriers or service providers may charge fees for data usage, messaging, phone calls or other services that are required for them to use the Services.

5.2 Customer's Order Form will indicate an initial allotment of Telephony Credits, if applicable. Customer may purchase additional Telephony Credits separately via the billing section of the Duo Admin Panel or by contacting a sales representative. U.S. and international rates for telephony can be found at https://www.duo.com/docs/telephony_credits.

5.3 If a Customer uses only Free Services, Duo Security will not charge such Customer any Fees for use of such Free Services or download, installation or use of the Software associated with Free Services. Such Customer may discontinue using the Free Services at any time, but must immediately remove any Software from its devices.

5.4 At any time during the Term, and unless otherwise agreed to in writing by the parties, any increase or overage in the maximum number of Users specified in the Order Form will be treated in accordance with this Section 5.4 (a "Subscription Upgrade"). The maximum number of Users shall be increased as follows:

For Subscription Upgrades (i) for Customers where the maximum number of Users on the Order Form is fewer than 500 Users, the maximum number of Users will be increased automatically in increments equal to 50 Users, (ii) for Customers where the maximum number of Users on the Order Form is 500 - 1000 Users, the maximum number of Users will be increased automatically in increments equal to 100 Users, and (iii) for Customers where the maximum number of Users on the Order Form is 1001 or greater, the maximum number of Users will be increased automatically in increments equal to 250 Users.

Duo Security shall invoice Customer for the increase in the maximum number of Users at the subscription rate and payment terms specified in the most recent Order Form, prorated for the remainder of the then applicable subscription Term. For any future subscription Term, the number of Users and applicable Fees will reflect any Subscription Upgrades.

6. CONFIDENTIALITY

6.1 The term “Confidential Information” means any information disclosed by one party (“Disclosing Party”) to the other party (“Receiving Party”) in any form (written, oral, etc.) that is marked as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of the disclosure, including, without limitation: trade secrets; technology and technical information (intellectual property, inventions, know-how ideas and methods); business, financial and customer information (including Customer Data and Customer Personal Data); pricing, forecasts, strategies and product development plans; and/or the terms of this Agreement. Each party understands that the Disclosing Party has or may disclose Confidential Information in connection with this Agreement, but that Receiving Party shall receive no rights in, or licenses to, such Confidential Information.

6.2 The Receiving Party agrees: (i) not to disclose Confidential Information to any third person other than those of its employees, contractors, advisors, investors and potential acquirers (“Representatives”) with a need to have access thereto and who have entered into non-disclosure and non-use agreements applicable to the Disclosing Party’s Confidential Information, and (ii) to use such Confidential Information solely as reasonably required in connection with the Services and/or this Agreement. Each party agrees to be responsible for any breach of this Agreement caused by any of its Representatives. The Receiving Party further agrees to take the same security precautions to protect against unauthorized disclosure or unauthorized use of such Confidential Information of the Disclosing Party that the party takes with its own confidential or proprietary information, but in no event will a party apply less than reasonable precautions to protect such Confidential Information. Each party acknowledges that the use of such precautions is not a guarantee against unauthorized disclosure or use. The Disclosing Party agrees that the foregoing will not apply with respect to any information that the Receiving Party can document: (a) is or becomes generally available to the public without any action by, or involvement of, the Receiving Party; or (b) was in its possession or known by it prior to receipt from the Disclosing Party; or (c) was rightfully disclosed to it without restriction by a third party; or (d) was independently developed without use of any Confidential Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing Confidential Information as required in response to a request under applicable open records laws or pursuant to any judicial or governmental order, provided that, to the extent permitted by law, the Receiving Party gives the Disclosing Party reasonable prior notice to contest such disclosure. For the avoidance of doubt, Customer acknowledges that Duo Security utilizes the services of, and Customer may request additional services from, certain third parties in connection with Duo Security’s provision of the Services (such as data hosting and telephony service providers and Customer’s Third Party

Services providers) and such third parties will have access to Customer's Confidential Information, including Customer Data in accordance with this Agreement. The parties agree that Performance Data is not Confidential Information and will not be subject to any confidentiality restrictions or obligations.

6.3 Each party agrees that, upon the written request of the Disclosing Party, the Receiving Party will promptly return to the Disclosing Party, or provide written certification of the destruction of, all Confidential Information of the Disclosing Party, including all Confidential Information contained in internal documents, without retaining any copy, extract or summary of any part thereof. Notwithstanding the foregoing, a Receiving Party may retain copies of Confidential Information solely to the extent necessary for purposes of such party's ordinary course internal document retention and backup requirements and procedures, provided that such Confidential Information shall remain subject to the terms and conditions of this Agreement for so long as it is retained.

6.4 Customer acknowledges that Duo Security does not wish to receive any Confidential Information from Customer that is not necessary for Duo Security to perform its obligations under this Agreement, and, unless the parties specifically agree otherwise, Duo Security may reasonably presume that any unrelated information received from Customer is not confidential or Confidential Information, unless such information is marked as "Confidential."

7. INTELLECTUAL PROPERTY RIGHTS; OWNERSHIP

Except as expressly set forth herein, Duo Security alone (and its licensors, where applicable) will retain all Intellectual Property Rights relating to the Services or the Software or any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Customer or any third party relating to the Services and/or the Software, which are hereby assigned to Duo Security. Customer will not copy, distribute, reproduce or use any of the foregoing except as expressly permitted under this Agreement. As between the parties, Duo Security owns all Performance Data. This Agreement is not a sale and does not convey to Customer any rights of ownership in or related to the Services or Software, or any Intellectual Property Rights.

8. DATA PROTECTION

8.1 In this Section 8, the terms "personal data," "data processor," "data subject," "process and processing" and "data controller" shall be as defined in the applicable Data Protection Laws. For the purposes of the Data Protection Laws, as between Customer and Duo Security, the parties agree that Customer shall at all times be the data controller and Duo Security shall be the data processor with respect to the processing of Customer Personal Data in connection with Customer's use of the Services. Solely if and to the extent Duo Security is processing personal data, as defined in the General Data Protection Regulation, that is contained in Customer Data on Customer's behalf, then the terms of the data processing agreement available at https://duo.com/legal/gdpr-data-protection-addendum shall apply to such processing and are incorporated into this Agreement.

8.2 Customer may enable integrations between the Services and certain of its Third Party Services (each, an “Integration”). By enabling an Integration between the Services and its Third Party Services, Customer is expressly instructing Duo Security to share the Customer Data necessary to facilitate the Integration. Customer is responsible for providing any and all instructions to the Third Party Service provider about the use and protection of Customer Data. Duo Security and Third Party Service providers are not subprocessors of each other.

8.3 As the data controller of Customer Personal Data, Customer represents and warrants to Duo Security that its provision of personal data to Duo Security and instructions for processing such personal data in connection with the Services shall comply with all Data Protection Laws.

8.4 In accordance with applicable Data Protection Laws, Duo Security shall take all commercially reasonable measures to protect the security and confidentiality of Customer Personal Data against any accidental or illicit destruction, alteration or unauthorized access or disclosure to third parties. Duo Security will provide Customer with its security policy, upon request, that sets forth the technical specifications and the detailed measures taken to protect the security and confidentiality of Customer Personal Data.

8.5 Customer may, upon at least thirty (30) days prior notice, and no more than once per 12 month period, appoint an independent third party auditor to physically inspect and audit, at Customer’s sole cost and expense, any facilities owned or controlled by Duo Security in which Customer Personal Data is processed or stored, provided that such inspection: (i) shall occur on a mutually agreed upon date during Duo Security’s regular business hours; (ii) does not interfere with any of Duo Security’s business operations; and, (iii) does not, in Duo Security’s reasonable discretion, create any risk to the confidentiality, integrity, or availability of any data stored or processed by Duo Security. Prior to any audit, Customer, and any appointed auditor, must enter into a nondisclosure and confidentiality agreement as may be required by Duo Security.

9. INDEMNIFICATION

For Customers enrolled in one of the editions of Services requiring purchase, Duo Security shall indemnify and hold Customer harmless from liability to third parties resulting from infringement by the Services of any patent or any copyright or misappropriation of any trade secret, provided Duo Security is promptly notified of any and all threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume sole control over defense and settlement; Duo Security will not be responsible for any settlement it does not approve. The foregoing obligations do not apply with respect to portions or components of the Services (i) not created by Duo Security, (ii) resulting in whole or in part from Customer specifications, (iii) that are modified after delivery by Duo Security, (iv) combined with other products, processes or materials where the alleged infringement relates to such combination, (v) where Customer continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (vi) where Customer’s use of Services is not strictly in accordance with this Agreement and all related Documentation. If Duo Security receives information about an actual or alleged infringement or misappropriation claim that would be subject to indemnification rights set forth in this Section 9, Duo Security shall have the option, at its expense, to: (a) modify the Software to be non-infringing; or (b) obtain for Customer a license to continue using the Software. If Duo Security determines it is not commercially reasonable to perform either of the above options, then Duo Security may at its option elect to terminate the license for the Services and refund the unearned portion of any pre-paid subscription Fees, prorated on a monthly basis. THIS SECTION STATES CUSTOMER’S SOLE AND EXCLUSIVE REMEDY FOR INFRINGEMENT, MISAPPROPRIATION AND/OR CLAIMS ALLEGING INFRINGEMENT OR MISAPPROPRIATION. Customer will indemnify Duo Security from all damages, costs, settlements, attorneys’ fees and expenses related to any claim related to Customer’s breach of Section 3 “Customer Responsibilities,” Section 4 “Restrictions,” Section 7 “Intellectual Property Rights; Ownership” or Section 8 “Data Protection.” Duo Security’s obligations under this Section 9 do not apply to Customer’s use of Free Services.

10. TERM; TERMINATION

10.1 Subject to earlier termination as expressly provided for in this Agreement, the initial Term of this Agreement shall be for the Term specified in the Order Form, or in the event of multiple Order Forms, until the Term of all Order Forms has expired. Each Order Form and this Agreement shall automatically renew after the initial Term and any renewal Term for a renewal Term equal to the expiring subscription Term, unless either party provides to the other at least forty-five (45) days prior written notice that it will not renew. The Fees per User for each renewal Term will be equal to the Fees per User for the immediately prior Term, plus a price increase. Any pricing increase will not exceed seven percent (7%) per year, unless the pricing was designated in the applicable Order Form as promotional or one-time; provided, however, the Fees for each renewal Term shall not exceed the list price as of the start date of such renewal Term.

10.2 In the event of any material breach of this Agreement by either party (other than Customer’s payment obligations), the non-breaching party may terminate this Agreement prior to the end of the Term by giving thirty (30) days prior written notice to the breaching party; provided, however, that this Agreement will not terminate if the breaching party has cured the breach prior to the expiration of such thirty-day period. If Customer fails to pay any Fees or other amounts in the applicable Order Form in accordance with the Payment Schedule, Duo Security may terminate this Agreement prior to the end of the Term by giving five (5) business days prior written notice to Customer; provided, however, that this Agreement will not terminate if Customer has paid all Fees and other amounts in the applicable Order Form prior to the expiration of such five business-day period.

10.3 Either party may terminate this Agreement, without notice, (i) upon the institution or if a petition is filed, notice is given, a resolution is passed or an order is made, in each case by or against the other party under Applicable Law relating to insolvency, administration, liquidation, receivership, bankruptcy or any other winding up proceedings, (ii) upon the other party's making an assignment for the benefit of creditors or making a voluntary arrangement with its creditors, (iii) upon the other party's dissolution or ceasing, or threatening to cease to do business or (iv) if any event occurs, or proceeding is instituted, with respect to the other party that has the equivalent or similar effect to any of the events mentioned in Section 10.3(i) through (iii). Notwithstanding anything in this Agreement to the contrary, Duo Security may, without penalty or liability and with or without notice, modify or discontinue its provision of Free Services at any time and to the extent Customer is only using Free Services immediately terminate this Agreement.

10.4 The Sections of this Agreement which by their nature should survive termination or expiration of this Agreement, including but not limited to Sections 3 through 14, will survive termination or expiration of this Agreement. No refund of Fees shall be due in any amount on account of termination by Duo Security pursuant to this Section 10. In the event of termination by Customer pursuant to this Section 10, Customer shall be entitled as its sole and exclusive remedy, to receive a refund of any pre-paid subscription Fees paid by Customer to Duo Security for Services not rendered as of the termination date. When this Agreement expires or terminates, Duo Security shall cease providing the Services to Customer.

11. WARRANTIES AND DISCLAIMER OF ADDITIONAL WARRANTIES

11.1 For Customers enrolled in one of the editions of Services requiring purchase, Duo Security represents and warrants that it will not knowingly include, in the Services released to Users and provided to Customer hereunder, any computer code or other computer instructions, devices or techniques, including without limitation those known as viruses, disabling devices, trojans, or time bombs, that intentionally disrupt, disable, harm, infect, defraud, damage, or otherwise impede in any manner, the operation of a network, computer program or computer system or any component thereof, including its security or User data. If, at any time, Duo Security fails to comply with the warranty in this Section 11.1, Customer may promptly notify Duo Security in writing of any such noncompliance. Duo Security will, within thirty (30) days of receipt of such written notification, either correct the noncompliance or provide Customer with a plan for correcting the noncompliance. If the noncompliance is not corrected or if a reasonably acceptable correction plan is not established during such period, Customer may terminate this Agreement and receive a refund of any pre-paid but unearned subscription Fees, prorated on a monthly basis, as its sole and exclusive remedy for such noncompliance. This provision does not apply to Customer's use of Free Services.

11.2 For Customers that have purchased Hardware Tokens as part of the Services, Duo Security warrants to Customer only that Hardware Tokens will be free of hidden defects in material and workmanship at the time of sale and for a period of six (6) months thereafter. This warranty is limited to replacement of defective Hardware Tokens. This Hardware Token warranty is Customer's exclusive remedy for defective Hardware Tokens. This provision does not apply to Customers who use only

Free Services.

11.3 EXCEPT AS EXPLICITLY PROVIDED IN THIS SECTION 11, THE SERVICES AND DUO SECURITY CONFIDENTIAL INFORMATION AND ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT ARE PROVIDED “AS-IS,” WITHOUT ANY WARRANTIES OF ANY KIND. DUO SECURITY HEREBY DISCLAIMS FOR ITSELF AND ITS SUPPLIERS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE, AND NON-INFRINGEMENT.

12. LIMITATION OF LIABILITY

12.1 NOTHING IN THIS AGREEMENT (OR ANY ORDER FORM) SHALL LIMIT OR EXCLUDE EITHER PARTY’S LIABILITY FOR (I) DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE, OR THE NEGLIGENCE OF ITS EMPLOYEES, AGENTS OR SUBCONTRACTORS; (II) FRAUD OR FRAUDULENT MISREPRESENTATION; (III) ITS INDEMNIFICATION OBLIGATIONS; (IV) BREACH OF SECTION 4 “RESTRICTIONS,” SECTION 5 “PAYMENT OF FEES,” OR SECTION 7 “INTELLECTUAL PROPERTY RIGHTS; OWNERSHIP” OR (V) ANY OTHER LIABILITY THAT CANNOT BE EXCLUDED OR LIMITED BY LAW.

12.2 SUBJECT TO SECTION 12.1, IN NO EVENT WILL EITHER PARTY OR THEIR SUPPLIERS BE LIABLE TO THE OTHER PARTY (OR ANY PERSON CLAIMING THROUGH SUCH PARTY) FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE OF THE SERVICES OR ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT, THE DELAY OR INABILITY TO USE THE SERVICES OR ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT OR OTHERWISE ARISING FROM THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, (I) LOSS OF REVENUE OR ANTICIPATED PROFITS (WHETHER DIRECT OR INDIRECT) OR (II) LOST BUSINESS OR (III) LOST SALES, WHETHER BASED IN CONTRACT, TORT (INCLUDING ACTIVE AND PASSIVE NEGLIGENCE AND STRICT LIABILITY) BREACH OF STATUTORY DUTY OR OTHERWISE, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES.

12.3 SUBJECT TO SECTION 12.1, THE MAXIMUM LIABILITY OF EITHER PARTY OR THEIR SUPPLIERS FOR ANY AND ALL CLAIMS UNDER AN APPLICABLE ORDER FORM, WHETHER BASED IN CONTRACT, TORT (INCLUDING ACTIVE AND PASSIVE NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE, WILL NOT EXCEED, IN THE AGGREGATE, THE FEES PAID OR TO BE PAID TO DUO SECURITY UNDER SUCH ORDER FORM DURING THE TWELVE MONTH PERIOD ENDING ON THE DATE THAT SUCH CLAIM IS FIRST ASSERTED. THE FOREGOING LIMITATION WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

13. GOVERNMENT MATTERS

13.1 Export. Notwithstanding anything else in this Agreement, Customer may not use, or provide to any person or export or re-export or allow the export or re-export of, the Services or anything related thereto or any direct product thereof, in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority. Each party represents that it is not named on any U.S. government denied-party list. Customer and Users shall not access or use the Services in a U.S. embargoed country.

13.2 Anti-Corruption. Customer agrees that it has not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any Duo Security employee or agent in connection with this Agreement. If Customer learns of any violation of the above restriction, Customer will promptly notify Duo Security.

13.3 Commercial Software. The Services (including the Software) are “commercial items” as that term is defined at FAR 2.101. If acquired by or on behalf of any Executive Agency (other than an agency within the Department of Defense (DoD), the Government acquires, in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software), only those rights in technical data and software customarily provided to the public as defined in this Agreement. If acquired by or on behalf of any Executive Agency within the DoD, the Government acquires, in accordance with DFARS 227.7202-3 (Rights in commercial computer software or commercial computer software documentation), only those rights in technical data and software customarily provided in this Agreement. In addition, DFARS 252.227-7015 (Technical Data – Commercial Items) applies to technical data acquired by DoD agencies. Any Federal Legislative or Judicial Agency shall obtain only those rights in technical data and software customarily provided to the public as defined in this Agreement. This Section 13.3 is in lieu of, and supersedes, any other FAR, DFARS, DEAR or other clause, provision, or supplemental regulation that addresses Government rights in computer software or technical data under this Agreement. Capitalized terms used in this Section are defined in the applicable FAR or DFARs.

14. MISCELLANEOUS

14.1 Severability. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

14.2 Assignment. This Agreement is not assignable, transferable or sublicensable by Customer except with Duo Security’s prior written consent, which shall not be unreasonably withheld. Duo Security may transfer and assign any of its rights and obligations under this Agreement. This Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their respective permitted successors and permitted assigns.

14.3 No Third Party Beneficiaries. Nothing in this Agreement shall confer, or is intended to confer, on any third party any benefit or the right to enforce any term of this Agreement. No entities other than Duo Security and Customer may terminate, rescind or agree to any modification, waiver or settlement with respect to this Agreement.

14.4 Entire Agreement; Amendment. Both parties agree that this Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement. All waivers, amendments and modifications must be in writing signed by the party against whom the waiver, amendment or modification is to be enforced; however, there will be no force or effect given to any different or additional terms contained in any purchase order or other vendor form issued by Customer, even if signed by Duo Security after the date hereof. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Customer does not have any authority of any kind to bind Duo Security in any respect whatsoever.

14.5 Notices. All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by e-mail; and upon receipt, if sent by certified or registered mail (return receipt requested), postage prepaid. Duo Security may provide notice using the information provided in the most recent Order Form and Customer may provide notice using the contact information provided on https://www.duo.com.

14.6 Force Majeure. Any delay or failure in the performance of any duties or obligations of either party (except the payment of money owed) will not be considered a breach of this Agreement if such delay or failure is due to a labor dispute, fire, earthquake, flood or any other event beyond the reasonable control of a party, provided that such party promptly notifies the other party thereof and uses reasonable efforts to resume performance as soon as possible.

14.7 Governing Law; Arbitration. This Agreement will be governed by the laws of the State of Michigan, U.S.A. without regard to its conflict of laws provisions. Any dispute arising from or relating to the subject matter of this Agreement shall be finally settled by arbitration in Washtenaw County, Michigan, in accordance with the Streamlined Arbitration Rules and Procedures of Judicial Arbitration and Mediation Services, Inc. ("JAMS") then in effect, by one commercial arbitrator with substantial experience in resolving intellectual property and commercial contract disputes, who shall be selected from the appropriate list of JAMS arbitrators in accordance with the Streamlined Arbitration Rules and Procedures of JAMS. Judgment upon the award so rendered may be entered in a court having jurisdiction, or application may be made to such court for judicial acceptance of any award and an order of enforcement, as the case may be. Notwithstanding the foregoing, each party shall have the right to institute an action in a court of proper jurisdiction for injunctive or other equitable relief pending a final decision by the arbitrator.

14.8 Venue; Prevailing Party. The federal and state courts sitting in Washtenaw County, Michigan, U.S.A. will have proper and exclusive jurisdiction and venue with respect to any disputes arising from or related to the subject matter of this Agreement. Notwithstanding the foregoing, each party shall have the right to commence and prosecute any action for injunctive relief before any court of competent jurisdiction. In any arbitration, action or proceeding to enforce rights under this Agreement, the prevailing party will be entitled to recover costs and attorneys' fees.

14.9 Publicity. Customer agrees to participate in press announcements, case studies, trade shows, or other marketing reasonably requested by Duo Security. During the Term and for thirty (30) days thereafter, Customer grants Duo Security the right, free of charge, to use Customer's name and/or logo, worldwide, to identify Customer as such on Duo Security's website or other marketing or advertising materials.

Contact Support

support@duo.com

Call Sales

1.866.760.4247

Email Sales

Contact Sales

Multi-Factor Authentication (MFA)

Duo Mobile

Authentication Methods

Phishing Simulator

Endpoint Visibility

Unified Endpoint Visibility

Trusted Endpoints

Endpoint Remediation

Self-Remediation

Use Cases

Education

Federal

Financial

Healthcare

Legal

Retail

Technology

Case Studies

Etsy

Threadless

Resources

Ebooks

Videos

Infographics

Events & Webinars

InfoSec Glossary

Phishing Tool

Support

Documentation

Knowledge Base

Status

About Duo

Blog

Careers

Culture

Press

Contact Us

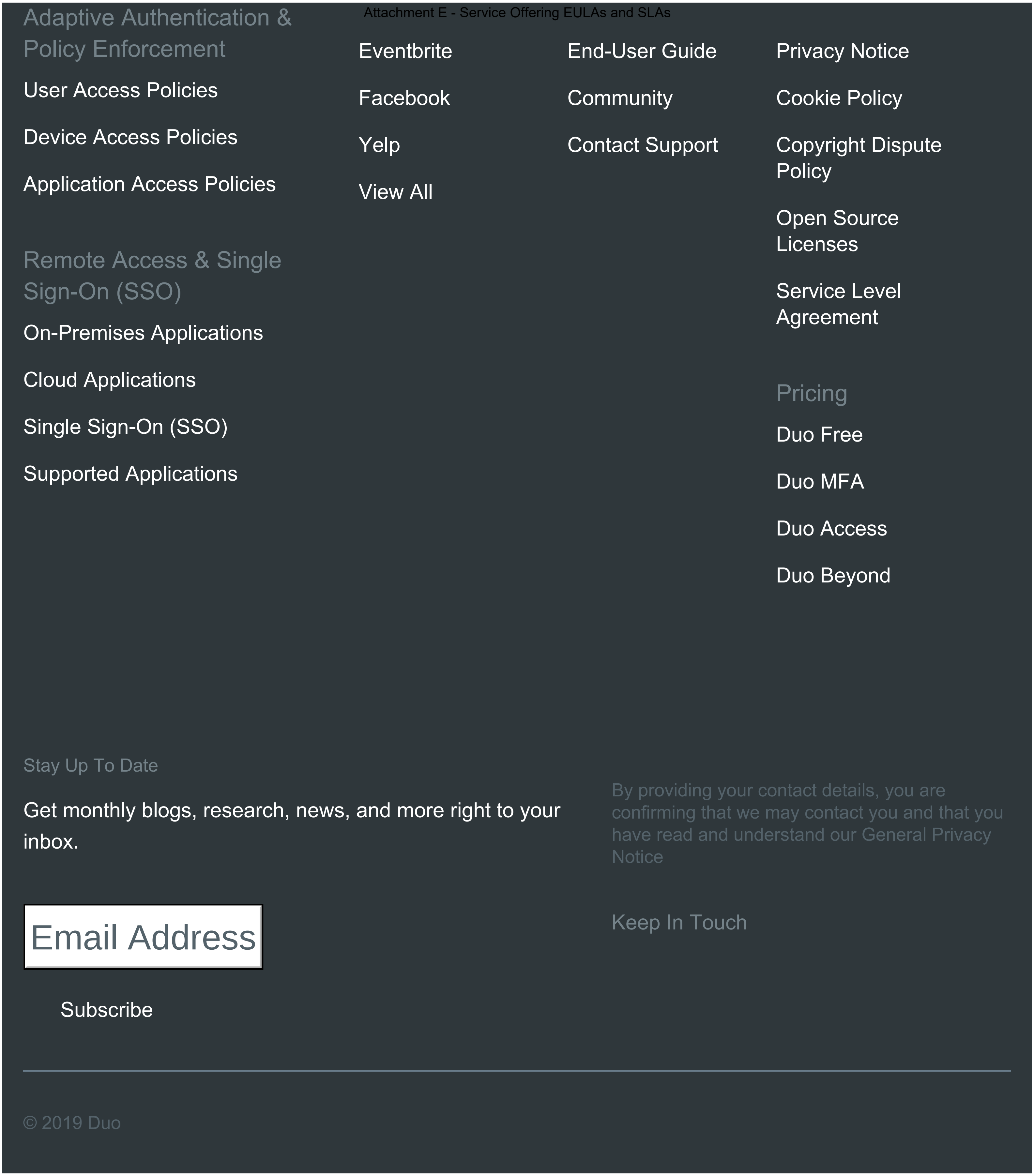
MSP Program

Disclosure Policy

Security Response

Legal

Terms of Service



Adaptive Authentication & Policy Enforcement

User Access Policies

Device Access Policies

Application Access Policies

Remote Access & Single Sign-On (SSO)

On-Premises Applications

Cloud Applications

Single Sign-On (SSO)

Supported Applications

Eventbrite

Facebook

Yelp

View All

End-User Guide

Community

Contact Support

Privacy Notice

Cookie Policy

Copyright Dispute Policy

Open Source Licenses

Service Level Agreement

Pricing

Duo Free

Duo MFA

Duo Access

Duo Beyond

Stay Up To Date

Get monthly blogs, research, news, and more right to your inbox.

By providing your contact details, you are confirming that we may contact you and that you have read and understand our General Privacy Notice

Keep In Touch

Duo Security is now a part of Cisco

Contact Sales

Free Trial

Service Level Agreement

EFFECTIVE AS OF JUNE 8TH, 2018

Duo Security SLA During the term of your Duo Security license (the "Agreement", the Duo web admin interface and web services will be operational and available to Customer at least 99.9% of the time in any calendar month (the "Duo Security SLA"). If Duo Security does not meet the Duo Security SLA, and if Customer meets its obligations under this Duo Security SLA, Customer will be eligible to receive the Service Credits described below. This Duo Security SLA states Customer's sole and exclusive remedy for any failure by Duo Security to meet the Duo Security SLA.

Definitions The following definitions shall apply to the Duo Security SLA.

- "Downtime" means when there is more than a five percent user error rate across all of a Customer's Users. Downtime is measured based on server side error rate.
- "Service" means the Duo Security multifactor authentication service.
- "Monthly Uptime Percentage" means total number of minutes in a calendar month minus the number of minutes of Downtime suffered in a calendar month, divided by the total number of minutes in a calendar month.
- "Service Credit" means the number of days of Service to be added to the end of the Service term, at no charge to Customer calculated as follows:

Uptime	Days Credited
< 99.95% - ≤ 99.9% (Duo Care premium only)	3
< 99.9% - ≤ 99.0%	3
< 99.0% - ≤ 95.0%	7
< 95.0%	15

Customer Must Request Service Credit In order to receive any of the Service Credits described above, Customer must notify Duo Security within thirty days from the time Customer becomes eligible to receive a Service Credit. Failure to comply with this requirement will forfeit Customer's right to receive a Service

Credit. Customer may check whether Duo Security's systems are operational by visiting https://status.duo.com.

Maximum Service Credit The aggregate maximum number of Service Credits to be issued by Duo Security to Customer for all Downtime that occurs in a single calendar month shall not exceed fifteen days of Service (or the value of 15 days of Service in the form of a monetary credit to a monthly-billing Customer's account). Service Credits may not be exchanged for, or converted to, monetary amounts.

Duo Security SLA Exclusions The Duo Security SLA does not apply to any services that expressly exclude this Duo Security SLA (as stated in the documentation for such services) or any performance issues: (i) caused by "Force Majeure" or (ii) that resulted from one or more of Customer's equipment or third party equipment not within the primary control of Duo Security.

Duo Security reserves the right to modify this Service Level Agreement at any time by updating the terms on this site.

Contact Support

support@duo.com

Call Sales

1.866.760.4247

Email Sales

Contact Sales

Multi-Factor Authentication (MFA)

Duo Mobile

Authentication Methods

Phishing Simulator

Endpoint Visibility

Unified Endpoint Visibility

Trusted Endpoints

Endpoint Remediation

Self-Remediation

Adaptive Authentication &

Use Cases

Education

Federal

Financial

Healthcare

Legal

Retail

Technology

Case Studies

Etsy

Threadless

Resources

Ebooks

Videos

Infographics

Events & Webinars

InfoSec Glossary

Phishing Tool

Support

Documentation

Knowledge Base

Status

About Duo

Blog

Careers

Culture

Press

Contact Us

MSP Program

Disclosure Policy

Security Response

Legal

Terms of Service

TREND MICRO END USER LICENSE AGREEMENT

Software/Service: Trend Micro Software Applications
Version: English/Multi-country
Date: August 2016

Important: The following Agreement sets forth the terms and conditions under which Trend Micro is willing to allow you, an individual or an authorized representative of an entity, to access and use the Software and/or online Software and Service. Read it carefully before deciding whether you accept or do not accept its terms.

BY SELECTING THE "I ACCEPT AGREEMENT" BUTTON OR BOX BELOW, YOU ARE EXPRESSING YOUR INTENT TO ENTER INTO, AND ARE ENTERING INTO, A BINDING LEGAL CONTRACT ("AGREEMENT") BETWEEN YOU AND TREND MICRO INCORPORATED OR ONE OF ITS AFFILIATES ("TREND MICRO"). THE TERMS AND CONDITIONS OF THE AGREEMENT THEN APPLY TO YOUR USE OF THE SOFTWARE AND SERVICE.

TREND MICRO RESERVES THE RIGHT TO AMEND THESE TERMS AT ANY TIME AT TREND MICRO'S SOLE AND EXCLUSIVE DISCRETION, BY POSTING SUCH CHANGES ON TREND MICRO'S MAIN WEBSITE, WWW.TRENDMICRO.COM. THE AMENDED TERMS SHALL BE EFFECTIVE AS OF THE DATE POSTED. IT IS YOUR RESPONSIBILITY TO CHECK THE WEBSITE TO LEARN OF THESE MODIFICATIONS. YOU AGREE TO BE BOUND TO THE TERMS OF THE AGREEMENT, AS MODIFIED. IF YOU DO NOT AGREE TO THE MODIFIED TERMS, YOU ARE NOT PERMITTED TO USE THE SOFTWARE AND SERVICE.

WE ENCOURAGE YOU TO PRINT A COPY OF THE AGREEMENT FOR YOUR RECORDS OR SAVE A COPY TO YOUR COMPUTER'S HARD DRIVE.

YOU MUST ACCEPT THIS AGREEMENT BEFORE YOU DOWNLOAD THE SOFTWARE AND ACCESS AND USE THE SERVICE. IF YOU ARE AN INDIVIDUAL, THEN YOU MUST BE AT LEAST 18 YEARS OLD AND HAVE ATTAINED THE AGE OF MAJORITY IN THE STATE, PROVINCE OR COUNTRY WHERE YOU LIVE TO ENTER INTO THIS AGREEMENT. IF YOU ARE USING THE SOFTWARE OR SERVICE ON BEHALF OF AN ENTITY, THEN YOU MUST BE PROPERLY AUTHORIZED TO REPRESENT THAT ENTITY AND TO ACCEPT THIS AGREEMENT ON ITS BEHALF.

IF YOU OR THE ENTITY YOU REPRESENT DOES NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT ACTIVATE OR USE THE SOFTWARE AND SELECT "I DO NOT ACCEPT THE AGREEMENT". THEN NO AGREEMENT WILL BE FORMED AND YOU WILL NOT BE PERMITTED TO ACCESS OR USE THE SOFTWARE AND SERVICE.

1. **LICENSE GRANT.** Subject to your acceptance and compliance with all terms of this Agreement, Trend Micro grants you a limited, revocable, personal, non-exclusive, non-transferable and non-sub-licensable right to download and install the Software and/or to access and use the Service as authorized by Trend Micro. Trend Micro reserves the right to enhance, modify, suspend or discontinue the Software and Service or to impose new or different conditions on their use at any time without notice.

2. **USE RESTRICTIONS.** The Software and/or Service are licensed and not sold. Trend Micro owns the title and intellectual property rights to the Software, Service and related documentation, and reserves all rights not expressly granted to you in this Agreement. You agree that you will not rent, loan, lease or otherwise make commercial use of the Software and/or Service or use them to provide services to others. You agree not to attempt to reverse engineer, decompile, modify, translate, disassemble, discover the source code of, or create derivative works from, any part of the Software and/or Service or authorize others to undertake any of these acts.

3. **BACK-UP AND ACKNOWLEDGEMENT**. For as long as you use the Software and/or Service, you agree regularly to back-up your Computer programs and files ("Data") on a separate media. You acknowledge that the failure to do so may cause you to lose Data in the event that any error in the Software and/or Service causes problems to your Computer or renders it inoperable, and that Trend

Micro is not responsible for any such Data loss. You agree that you are responsible for deciding if and how you use the Software and/or Service.

4. **INFORMATION COLLECTION.** Trend Micro may process and store certain information about your network and equipment to provide the Services, to improve its databases and develop or improve its products and Services. In the event, you provide Trend Micro with personally-identifiable information all such information shall be maintained in accordance with Trend Micro's Privacy Policy, as may be amended from time to time, which can be found at www.trendmicro.com. You agree that Trend Micro may (i) use uploaded data from installed Software to improve our products and their functionality and provide you the Services, for product analysis, and to detect malicious behavior, potentially fraudulent websites and other Internet security risks and to provide you with the latest threat protection; (ii) share data that has been identified as malicious or unwanted content with worldwide affiliates and security partners; and (iii) use and disclose uploaded data for analysis or reporting purposes. Trend Micro reserves the title, ownership and all rights and interests to any intellectual property or work product resulting from its use and analysis of such information.

5. **NO WARRANTY.** THE SOFTWARE AND SERVICE ARE PROVIDED "AS IS", "WITH ALL FAULTS", "AS AVAILABLE", AND WITHOUT WARRANTIES OF ANY KIND. YOUR USE OF THE SOFTWARE AND SERVICES ARE AT YOUR OWN RISK. TREND MICRO DOES NOT WARRANT THAT THE SOFTWARE OR SERVICE ARE SECURE OR ERROR FREE OR COMPLETE OR ACCURATE OR THAT THEY WILL DETECT, REMOVE OR CLEAN ALL, OR ONLY, MALICIOUS OR UNWANTED APPLICATIONS, CONTENT AND FILES. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, TREND MICRO AND ITS AFFILIATES AND SUPPLIERS HEREBY DISCLAIM AND EXCLUDE ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THE SOFTWARE AND SERVICE, EITHER EXPRESS, OR IMPLIED BY STATUTE, COMMON LAW OR TRADE USAGE, INCLUDING BUT NOT LIMITED TO WARRANTIES OR CONDITIONS OF TITLE, NONINFRINGEMENT OF THIRD PARTY RIGHTS, SATISFACTORY QUALITY, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

6. **NO LIABILITY FOR CONSEQUENTIAL DAMAGES.**

   (A) TREND MICRO DOES NOT SEEK TO LIMIT OR EXCLUDE ITS LIABILITY IN THE EVENT OF DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE OR FOR FRAUD OR FOR ANY OTHER LIABILITY FOR WHICH IT IS NOT PERMITTED BY LAW TO EXCLUDE.

   (B) SUBJECT TO SECTION (A) ABOVE, IN NO EVENT SHALL TREND MICRO BE LIABLE TO YOU (i) FOR ANY LOSSES WHICH WERE NOT REASONABLY FORSEEABLE AT THE TIME OF ENTERING INTO THIS AGREEMENT OR (ii) FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES OF ANY KIND OR FOR LOST OR CORRUPTED DATA OR MEMORY, SYSTEM CRASH, DISK/SYSTEM DAMAGE, LOST PROFITS OR SAVINGS, OR LOSS OF BUSINESS, ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE USE, MISUSE OR INABILITY TO USE SOFTWARE AND SERVICE, OR (iii) ANY DAMAGES IN EXCESS OF USD$50.00. THESE LIMITATIONS OF LIABILITY SHALL APPLY EVEN IF TREND MICRO OR ANY OF ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE FORM OF ACTION, WHETHER FOR BREACH OF CONTRACT, NEGLIGENCE, STRICT PRODUCT LIABILITY OR ANY OTHER CAUSE OF ACTION OR THEORY OF LIABILITY. YOU AGREE TO THE LIMITATIONS OF LIABILITY IN THIS SECTION AND ACKNOWLEDGE THAT WITHOUT YOUR AGREEMENT TO THIS PROVISION, TREND MICRO WOULD NOT BE ABLE TO OFFER YOU THE RIGHT TO USE THE SOFTWARE AND SERVICES AT NO CHARGE.

7. **INDEMNIFICATION.** YOU AGREE TO RELEASE AND INDEMNIFY TREND MICRO AND ITS AFFILIATES FROM AND AGAINST ANY AND ALL CLAIMS AND DAMAGES OF ANY KIND (INCLUDING ATTORNEYS' FEES) RESULTING FROM OR RELATING TO YOUR USE OR INTERACTION WITH THE SOFTWARE AND SERVICE OR FROM YOUR BREACH OF ANY PROVISION OF THIS AGREEMENT.

8. **CONSUMER AND DATA PROTECTION**. SOME COUNTRIES, STATES AND PROVINCES, INCLUDING MEMBER STATES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW CERTAIN EXCLUSIONS OR LIMITATIONS OF LIABILITY, SO THE ABOVE DISCLAIMER OF WARRANTY OR LIMITATION OF LIABILITIES (SECTIONS 5 AND 6) MAY NOT FULLY APPLY TO YOU. YOU MAY HAVE ADDITIONAL RIGHTS AND REMEDIES. SUCH RIGHTS OR REMEDIES, IF ANY, MAY NOT BE AFFECTED BY THIS AGREEMENT. NOTWITHSTANDING THE PROVISIONS IN THIS AGREEMENT, THERE MAY BE MANDATORY REGULATIONS OR LEGAL PROVISIONS THAT ARE APPLICABLE TO YOU AS A CONSUMER.

   YOU HEREBY GIVE YOUR CONSENT TO TREND MICRO TO PROCESS PERSONAL DATA PROVIDED BY YOU ("PERSONAL DATA") IN CONNECTION WITH THIS AGREEMENT; PROCESSING MAY INCLUDE COLLECTION, REGISTRATION, STORAGE, MODIFICATION OR DISCLOSURE OF SUCH PERSONAL DATA TO THIRD PARTIES. YOU ALSO GIVE YOUR CONSENT TO TREND MICRO TO TRANSFER YOUR PERSONAL DATA TO ONE OR MORE OF ITS GROUP COMPANIES, LOCATED IN AND/OR OUTSIDE THE EUROPEAN UNION/EUROPEAN ECONOMIC AREA, AND WHICH MAY HAVE A LOWER LEVEL OF PROTECTION OF PERSONAL DATA THAN IS APPLICABLE IN THE EU/EEA. SUCH TRANSFER WILL ONLY BE CARRIED OUT IN CONNECTION WITH THIS AGREEMENT, AS IS THE CASE WITH THE PROCESSING OF YOUR PERSONAL DATA BY THESE GROUP COMPANIES. TREND MICRO IS THE CONTROLLER OF PERSONAL DATA. IN THE EVENT YOU WOULD LIKE INFORMATION ON THE PERSONAL DATA THAT TREND MICRO PROCESSED FOR YOU OR IF YOU WISH TO HAVE IT CORRECTED OR MODIFIED, YOU MAY CONTACT TREND MICRO AT THE ADDRESS GIVEN BELOW.

9. **EXPORT CONTROL.** The Software is subject to export controls under the U.S. Export Administration Regulations. Therefore, the Software may not be exported or re-exported to entities within, or residents or citizens of, embargoed countries or countries subject to applicable trade sanctions, nor to prohibited or denied persons or entities without proper government licenses. Information about such restrictions can be found at the following websites: http://www.treas.gov/ofac/ and www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm. As of the Date above, countries embargoed by the U.S. include Cuba, Iran, North Korea, Sudan and Syria. You are responsible for any violation of the U.S. export control laws related to the Software. By accepting this Agreement, you confirm that you are not a resident or citizen of any country currently embargoed by the U.S. and that you are not otherwise prohibited from receiving the Software.

10. **U.S. GOVERNMENT RESTRICTED RIGHTS.** This Software is "Commercial Computer Software" as defined under DFARS 252.227-7014. If you are subject to the Defense Federal Acquisition Regulations (DFAR), and the Commercial Computer Software and associated documentation are sold pursuant to Trend Micro's standard commercial license pursuant to DFARS 227-7202-1, Commercial Products. For all other government customers, use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in FAR 52.227-19, as applicable.

11. **TERMINATION.** Trend Micro may terminate your rights under this Agreement immediately and without notice if you fail to comply with any term or condition of this Agreement. Upon such termination, you agree to delete or destroy all copies of the Software and stop using the Software and Service. You may terminate this Agreement at any point by destroying or deleting all copies of the Software. Trend Micro reserves the right to suspend or terminate your access or use of the Software and/or Service to prevent unauthorized access to or use of, or the misuse or inappropriate use of, the Software and/or the Service.

12. **GOVERNING LAW/JURISDICTION.** This Agreement will be governed by and construed in accordance with the laws of the State of California and the United States, without giving effect to the conflict of laws' provisions of California or Your actual state or country of residence. The exclusive jurisdiction and venue of any action with respect to the subject matter of this Agreement shall be the state courts of the State of California for the County of Santa Clara or the United States District Court for the Northern District of California and each of the parties hereto submits itself to the exclusive jurisdiction and venue of such courts for the purpose of any such action. The United Nations

Convention on Contracts for the International Sale of Goods do not apply to this Agreement under the laws of any country. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, the remainder of this Agreement will continue in full force and effect. Without limiting its rights and remedies at law and equity, Trend Micro shall have the right to seek an injunction and similar equitable relief in any appropriate forum to stop and/or prevent any unauthorized use or distribution of the Software and/or Intellectual Property rights contained in the Software.

13. **GENERAL.** This Agreement is the entire agreement between you and Trend Micro and supersedes any prior agreement or understanding, whether written or oral, relating to the subject matter of this Agreement. In the event that any provision of this Agreement is found invalid, that finding will not affect the validity of the remaining parts of this Agreement. Trend Micro may assign or subcontract some or all of its obligations under this Agreement to qualified third parties or its affiliates and/or subsidiaries, provided that no such assignment or subcontract shall relieve Trend Micro of its obligations under this Agreement.

14. **QUESTIONS.** Visit www.trendmicro.com/support/consumer if you have a question about the Software or Service. Direct all questions about this Agreement to: legal_notice@trendmicro.com.

THE SOFTWARE IS PROTECTED BY INTELLECTUAL PROPERTY LAWS AND INTERNATIONAL TREATY PROVISIONS. UNAUTHORIZED REPRODUCTION OR DISTRIBUTION IS SUBJECT TO CIVIL AND CRIMINAL PENALTIES.

TREND MICRO DEEP SECURITY AS A SERVICE

EULA Click Here

SERVICE LEVEL AGREEMENT

1. Purpose

This document describes the services and conditions related to the Trend Micro Deep Security As Service and does not apply to, nor describes, any other Trend Micro product or service.

The use of the Trend Micro Deep Security As a Service is subject to acceptance of and agreement to the terms and conditions of the applicable License Agreement (the "License Agreement") of Trend Micro Incorporated or an authorized affiliate (each "Trend Micro"). This document shall be an integral part of such License Agreement. The terms and conditions of the Trend Micro License Agreement shall apply to the use of the Service described in this document. In the event of a conflict between the terms of the License Agreement and those of this document, those of this document will prevail. All other terms and conditions of the License Agreement will remain in full force and effect.

2. Service Description

The Trend Micro Deep Security As a Service is a server (VM or Instance) and application protection management service offered by Trend Micro and is referred to herein as the "**Service**". The Service provides protection and centralized security policy management for supported cloud providers. It also provides policy-based protection for servers running on IaaS cloud environments and combines a management console with software agents deployed in each cloud server. The Service allows customers to set rules based on the virtual machine information where the software agents are installed to check for specific virtual machine attributes.

3.1 Customers must have an environment that has Internet access in order to use the Service.

3. Conditions of the Service

3.2 Customers must ensure Firewall Access Control Lists (**ACLs**) are configured to allow communication from certain IP ranges as specified by the applicable documentation for the Service.

3.3 Customers must have access to a browser application supported by the Service to use the Web-based administrative console.

3.4 Customers understand and agree that their security policies and security events are also logged or recorded by Trend Micro.

3.5 Customers must take all necessary measures to ensure that they and all of their employees are aware of and in compliance with any requirements, responsibilities and limitations set forth in any applicable data privacy and data protection laws, rules, and regulations.

4 Service Availability

4.1 The Service is hosted twenty-four (24) hours a day, seven (7) days a week in Trend Micro's managed public IaaS environment. The Service systems, network, and capacity are continually monitored to provide optimal availability and efficiency to Service customers.

4.2 Subject to applicable law, Trend Micro may provide any part of the Service from any cloud provider data center (region) anywhere in the world. In addition, at any time and for any reason, Trend Micro may transfer the Service provided to the customer from one cloud provider data center to another. Trend Micro does not guarantee that any cloud provider data center, or part thereof, is dedicated to the sole use of the customer, unless otherwise specified in writing.

4.3 In connection with the registration of new Agents and assigning/updating security policies from the Deep Security Agent running on the customer's environment to the Service, "**Service Availability**" pertains to and means the Service's availability to receive heartbeat and communication requests from customer's Deep Security Agent, subject to the correct configuration by the customer of its firewall, as necessary, and other requirements and guidelines set forth in Trend Micro's applicable documentation.

4.4 Trend Micro is committed in providing the highest level of service available. Trend Micro's datacenter operates in multi datacenter availability zones with multiple redundant backup instances. Trend Micro will use commercially reasonable efforts to provide the Service on a 24 hours a day, 7 days a week basis. However, as described in this document, the Service may be unavailable due to Scheduled Maintenance, unscheduled downtime or unforeseen circumstances including suspension of the Service to mitigate any malicious activities; in each such case, Trend Micro shall use commercially reasonable efforts to reinstate the Service as soon as possible.

4.5 Scheduled Maintenance of the Service will occur periodically to ensure on-going efficiency. To the extent possible, Trend Micro shall give customers at least seven (7) days' notice of any "**Scheduled Maintenance**" which may cause disruption of the Service, including unavailability of the Service. Whenever commercially reasonable, Scheduled Maintenance will be conducted without affecting the Service provided to customers. Scheduled Maintenance shall not exceed more than eight (8) hours per calendar month. Whenever commercially reasonable, Scheduled Maintenance: (a) will be conducted during periods of anticipated low new activation requests or security policy creations/edits/updates request traffic and (b) will be conducted on part, but not all, of the network at any one time to minimize the disruption to the Service.

4.6 Unscheduled downtime is defined as those times when the Service is unavailable and not able to process new activation requests or creation/edit/updating of policy requests. This does not include those times when the Service is undergoing Scheduled Maintenance as described in section 4.5 above. Trend Micro will inform customers as quickly as possible following the onset of unscheduled downtime.

4.7 If at any time the continued availability of the Service would compromise the security of the Service due to, but not limited to, hacking attempts, denial of service attacks, or other malicious activities either directed at or originating from the customer's environment, Trend Micro may temporarily suspend the Service as to such customer. In such an event, Trend Micro will promptly inform the customer and will work with the customer to resolve such issues, reinstating the Service at the earliest opportunity.

5 Privacy Policy

5.1 Security event information communications are routed through the Service and are entirely automated so there is no human intervention.

5.2 As part of the Service account registration, the customer is required to provide their email address. The customer email address is used as the username to login to the Service and is stored by the system.

5.3 To resolve a technical support problem, Trend Micro may request certain customer log files from the customer environment to help identify the problem. With the consent of and at the direction of the customer, Trend Micro may review such files to address customer's issue. Trend Micro will not otherwise access customer's files unless required by applicable law or pursuant to a court order or similar action.

6 Disaster Recovery

6.1 Trend Micro has a disaster recovery plan in connection with the Service. Because this is a Web-based Service, there may be events beyond the reasonable control of Trend Micro that may impact the Service ("Force Majeure Events"). However, to minimize the impact of these Force Majeure Events, the Service is based upon a geographically distributed, fully redundant system. If one data center becomes unavailable, the Service will fail over to a backup data center.

6.2 Disaster recovery procedures will be put into place under the following conditions:

6.2.1 A natural disaster or war situation that results in the primary data center hosting the Service not being able to serve customer requests for more than four (4) hours.

6.2.2 Any situation that results in the primary data center hosting the Service not being able to be accessed physically or remotely for more than four (4) hours by Trend Micro.

7 Technical Support and Customer Service

7.1 Customers may obtain technical support contact information by visiting the Trend Micro Deep Security As a Service support web page and selecting the appropriate region.

7.2 To receive prompt technical support, customer must provide the following information during the initial support call or email: Company Name, Administrator Account Name (but not the password), customer Contact Name, customer Contact Email Address, and a description of the issue. In addition, a copy of the license certificate should be included with online submissions (the license certificate information should also be available during phone support).

7.3 Customers that purchased a subscription to the Service through a channel partner should contact their channel partner for customer service requests regarding purchase order related queries, such as: (a) orders for the Service; (b) requests for modifications to the purchased service (*e.g*. changes to service management level, number of users, domains, etc.); and 3) billing and invoicing inquiries.

8 Modification

Trend Micro reserves the right to modify the Service and this document at any time without prior notice. The current version of this document can be found in the Trend Micro Deep Security As a Service administrative console for review by customers.