Contract #   AR2495

STATE OF UTAH COOPERATIVE CONTRACT

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

EMC Corporation			LEGAL STATUS OF CONTRACTOR
Name			☐ Sole Proprietor
2999 Douglas Blvd., Suite 275			☐ Non-Profit Corporation
Address			☒ For-Profit Corporation
Roseville	CA	95661	☐ Partnership
City	State	Zip	☐ Government Agency

Contact Person Pamela Kunhart Phone # (916) 797-7052_____ Email pamela.kunhart@dell.com
Vendor #_____ Commodity Code #920-05

2. **GENERAL PURPOSE OF CONTRACT:** Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed

3. **PROCUREMENT PROCESS:** This contract is entered into as a result of the procurement process on Bid#CH16012.

4. **CONTRACT PERIOD:** Effective Date: 09/30/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.

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

6. **ATTACHMENT A:** NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
   ATTACHMENT B: Scope of Services Awarded to Contractor
   ATTACHMENT C: Pricing Discounts and Pricing Schedule
   ATTACHMENT D: Contractor's Response to Solicitation #CH16012
   ATTACHMENT E:

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

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

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

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

CONTRACTOR		STATE	
signature	11/29/16	_signature_	11. 29. 2016
Contractor's signature	Date	Director, Division of Purchasing	Date
Joseph F. Spaniol, III			
Vice President Federal & Public Sector Contracts			
Type or Print Name and Title			

Christopher Hughes	801-538-3254		christopherhughes@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	Email
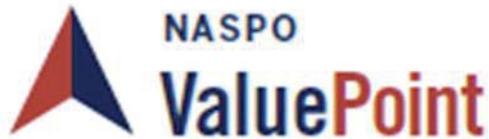
Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

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.

Affiliates means any entity that controls, is controlled by or is under common control with the Contractor.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential, that is disclosed or otherwise made available in the performance of this Master Agreement by either party to the other party, including by a Participating Entity or Purchasing Entity or each of their respective employees or agents, which information may, include, but not be limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, (4) technology, research and development information, Products, and software, and (5) trade secrets and other information which are competitive in nature

---

[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.

disclosed subject to state public records or comparable laws.

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, Fulfillment Partners and Affiliates who are providing the services agreed to under the Master Agreement.

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

Data Breach means any actual non-authorized access to or acquisition of computerized Non-Public Data or Personal Data in the Contractor's data center containing the Node or environment hosting Purchasing Entity's 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".

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 Purchasing Entity to provision processing, storage, networks, and other fundamental computing resources where the Purchasing Entity is able to deploy and run arbitrary software, which can include operating systems and applications. The Purchasing Entity 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, methodologies, ideas, concepts, inventions, know-how, techniques, 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 or that subsequently executes a Participating Addendum. 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 Purchasing Entity to deploy onto the cloud infrastructure Purchasing Entity -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 Purchasing Entity 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 Statement of Work that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the 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 in the Contractor's data center containing the Node or environment hosting Purchasing Entity's Data, 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 the service level for each of the cloud services provided by Contractor as set out in the description of such cloud services and incorporated herein or 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 Purchasing Entity to use the Contractor's applications running on 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 Purchasing Entity 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 as may be agreed to by Contractor and the Purchasing Entity that describes the services to be performed by Contractor for the Purchasing Entity, inclusive of Purchasing Entity's service needs and expectations.

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

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

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State; provided, Contractor may assign, sell, transfer or sublet rights or delegate responsibilities to a third party that acquires all or substantially all of its assets or a majority or controlling interest of its voting securities.

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 discount percentages off list price must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the benefit of the most current list price of the services provided under this Master Agreement. A price 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, as set out in this Master Agreement or any Participating Addendum, 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 and any responsibilities arising out of a Security Incident or Data Breach. If this Master Agreement, a Participating Addendum or and Order is terminated without cause prior to the expiration of the applicable order for the Services, the Purchasing Entity shall remain liable for the payment for the Services rendered prior to such termination and as may be agreed to by the parties, the payment to Contractor of the costs incurred by Contractor in purchasing the equipment used to provide the Service. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief
a. Confidentiality. Each party acknowledges that it and its employees or agents may, in the course of this Master Agreement, be exposed to or acquire information that is confidential to the other party, including 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 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 the receiving party) publicly known; (2) is furnished by the disclosing party to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in the receiving party's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than the disclosing party without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of the receiving party who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Each party shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, but no less that the standard of care such party uses for its own similar confidential information, 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. Each party shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Each party shall use commercially reasonable efforts to assist the disclosing party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, receiving party shall advise the disclosing party, including, as applicable the Purchasing Entity, applicable Participating Entity, and the Lead State immediately if the receiving party 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 the receiving party shall at its expense cooperate with the disclosing party in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by the disclosing party, the receiving party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at the disclosing party's request, the receiving party shall turn over to the disclosing party all documents, papers, and other matter in the receiving party's possession that embody Confidential Information. If applicable law, regulation or document retention policy prevents the receiving party from destroying or returning all or part of the Confidential Information the receiving party maintain the security and confidentiality of all such retained Confidential Information. Notwithstanding the foregoing, the receiving party 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, may 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, the non-breaching party shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days (or an additional period of time as may be agreed to by the parties) in which the other party shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its 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 either party's liability for damages.

c. If a party alleged to be in breach is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, such party shall be in breach of its obligations under this Master Agreement and the non-breaching party shall have the right to exercise any or all of the following remedies:

> (1) Exercise any remedy provided by law; and

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

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

> (4) Suspend Contractor's performance; and

> (5) Withhold payment 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 Master Agreement 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 real or tangible property arising directly from the solely negligent act(s), error(s), or omission(s) of the

Contractor, its employees or subcontractors, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. Contractor shall (i) at its own expense defend and indemnify the Lead State, Participating Entity or Purchasing Entity ("Indemnified Party") against any third party claim that a Product as provided by Contractor to the Purchasing Entity infringes a patent or copyright enforceable in a country that is a signatory to the Berne Convention; and (ii) pay the costs and damages to Indemnified Party that arise from the lawsuit as finally awarded against the Indemnified Party by a court of competent jurisdiction and to the extent that such are the result of the third party claim, or pay the amounts stated in a written settlement negotiated and approved by Contractor. The foregoing obligations are subject to the following: Indemnified Party (a) notifies Contractor within a reasonable time frame in writing of such claim;
(c) reasonably cooperates in response to a Contractor request for assistance and information; and (d) is not in material breach of this Master Agreement or Participating Addendum. The Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible.

Should any Product become, or in Contractor's opinion be likely to become, the subject of such a claim, Contractor may, at its option and expense, (1) procure for the Indemnified Party the right to make continued use thereof; (2) replace or modify such so that it becomes non-infringing so long as all material functionality is maintained; or (3) if, in Contractor's opinion, neither of the foregoing are reasonably available, Contractor shall notify the Purchasing Entity to return the Product and discontinue performance of the Service. If Contractor requests return of the Product or discontinuance of Service, Contractor shall refund the portion of any pre-paid fee that reasonably corresponds to the amount of Service no longer being performed. Contractor shall have no obligation or liability to the extent that the alleged infringement arises out of or relates to: (A) use or combination of Product with any technology, item(s) or services that Indemnified Party develops, owns or receives from a third party or any other technology or service not developed by Contractor, (B) use for a purpose or in a manner for which the Product was not designed; (C) any modification made by any person other than Contractor or its authorized representatives;(D) any modifications made by Contractor to the Product in accordance with the Indemnified Party's specifications or specific instructions; or (E) any Product made/performed by Contractor in accordance with Indemnified Party's instructions. (THIS SECTION STATES THE INDEMNIFIED PARTY'S SOLE AND EXCLUSIVE REMEDY AND EMC'S ENTIRE LIABILITY FOR INFRINGEMENT CLAIMS MADE AGAINST THE INDEMNIFIED PARTY.

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. Contractor will take commercially reasonable efforts to ensure such policies have a condition that they not be revoked by the insurer without thirty (30) calendar days' notice. Contractor will take commercially reasonable efforts to provide notice of revocation thereof unless the policy has been replaced.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a Certificate of Insurance that (1) names the Lead State as additional insured for General Liability and , (2) provides that all Participating States will be covered by such insurance policy without an additional process being required to add them, 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); Contractor will take commercially reasonable efforts to provide copies of renewal certificates of all required insurance 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. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

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

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

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement as an application service provider, service bureau or similar capacity for third parties. 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.

---

[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.

21. Payment: Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, its parent company, 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 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 solely and directly 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. Upon reasonable written notice and during Contractor's normal business hours, 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, access to Contractor's books, documents, papers and records solely and directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of audit inspection. This right shall survive for a period of six (6) years following termination of this Agreement.   Audits and audit results shall be treated as confidential by the Lead State, Participating Entity and Purchasing Entity, within the limits of the law including applicable public record laws.

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.

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, to the best of its knowledge and after utilizing commercially available virus-checking software, the Products it provides under this Master Agreement are free of malware, computer software viruses, worms, trap doors, back doors or other functions (collectively, "Virus") that detrimentally interferes with or otherwise adversely affects use of the Product. Upon detection of a Virus by a Purchasing Entity, Contractor shall be promptly notified and Purchasing Entity will use its best commercial efforts to mitigate against any damages or effects caused by the Virus. The Contractor will use reasonable commercial efforts to promptly eliminate such Virus, including industry-leading technology to detect and remove any Virus.   .

g. Warranty for Professional Services. Contractor shall perform Professional Services (defined as consulting, implementation, database/application administration, systems engineering and configuration services, training and other services) in a workmanlike manner in accordance with generally accepted industry standards. Unless otherwise agreed to in a Statement of Work, Purchasing Entity must notify Contractor in writing of

any failure to so perform within ten (10) days after the performance of the applicable portion of Professional Services.

Contractor's entire liability and Purchasing Entity's sole remedy for Contractor's failure to so perform shall be for Contractor to, at its option, (i) correct such failure; (ii) reperform the service, or (iii) terminate the applicable Statement of Work and refund that portion of any fees received that correspond to such failure to perform.

h. . **OTHER THAN AS EXPRESSLY SET FORTH IN THIS MASTER AGREEMENT, THE SERVICES, PRODUCT, PROFESSIONAL SERVICES AND OTHER MATERIALS PROVIDED BY CONTRACTOR HEREUNDER ARE PROVIDED "AS IS" AND CONTRACTOR AND ITS THIRD PARTY PROVIDERS DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICES, PRODUCT , PROFESSIONAL SERVICES AND OTHER MATERIALS PROVIDED UNDER THIS MASTER AGREEMENT OR ANY PARTICIPATING ADDENDUM, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COURSE OF PERFORMANCE OR USEASGE IN TRADE.**

32. Transition Assistance:

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

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 Contractor 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 must be in writing. A waiver by the of any default, right or remedy under this Master Agreement or Participating Addendum, with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or

requirement under this Master Agreement, Participating Addendum, or Purchase Order.

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

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c. 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.

d. 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.

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

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

44. Limitation of Liability.

a) EXCEPT WITH RESPECT TO CLAIMS PURSUANT TO SECTION 13 b. ABOVE, CONTRACTOR'S TOTAL LIABILITY UNDER THIS AGREMENT AND LEAD STATE, PARTICIPATING ENTITY OR PURCHASEING ENTITY'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM OF ANY TYPE WHATSOEVER, ARISING OUT OF PRODUCT OR SERVICE PROVIDED HEREUNDER, SHALL BE LIMITED TO PROVEN DIRECT DAMAGES CAUSED BY CONTRACTOR'S SOLE NEGLIGENCE IN AN AMOUNT NOT TO EXCEED (i) US$3,000,000, FOR DAMAGE TO REAL OR TANGIBLE PERSONAL PROPERTY; AND (ii) THE PRICE PAID TO CONTRACTOR FOR THE SPECIFIC SERVICE (CALCULATED ON AN ANNUAL BASIS, WHEN APPLICABLE) OR PRODUCT FROM WHICH SUCH CLAIM ARISES, FOR DAMAGE OF ANY TYPE NOT IDENTIFIED IN (i) ABOVE OR OTHERWISE EXCLUDED HEREUNDER. THE LIMITATION OF LIABILITY DOES NOT APPLY TO CONTRACTOR'S OBLIGATION TO INDEMNIFY FOR DEATH OR INJURY TO PERSON(S) AS IDENTIFIED IN SECTION 13a.

b) EXCEPT WITH RESPECT TO CLAIMS REGARDING VIOLATION OF CONTRACTOR'S INTELLECTUAL PROPERTY RIGHTS, NEITHER LEAD STATE, PARTICIPATING ENTITY, PURCHASING ENTITY NOR CONTRACTOR SHALL HAVE LIABILITY TO THE OTHER FOR ANY SPECIAL, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, REVENUES, DATA AND/OR USE), EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

c) Subject to applicable law, all claims must be made within (i) the time period specified by applicable law; or (ii) six 6 years after the cause of action accrues if no such period is specified at law

45. Use of Service

a) All use of the Services will comply with the Acceptable Use Policy for the Services set out in Exhibit 4 and located at http://www.virtustream.com/content/acceptable-use-policy.asp ("AUP"), which is incorporated herein by reference. Contractor may make reasonable changes to the AUP at any time and such change will be effective upon posting to the website or other notice to Purchasing Entity.

b) Purchasing Entity will not use, and will not authorize any third party to use any open source software in connection with the Services in any manner that requires, pursuant to the license applicable to such open source software, that any Confidential Information or Services be (i) disclosed or distributed in source code form, (ii) made available free of charge to recipients, or (iii) modifiable without restriction by recipients.

c) Contractor and/or its licensors own all Intellectual Property Rights in the Services. Except as expressly stated herein, this Agreement does not grant Purchasing Entity any rights to, or in, any Intellectual Property or any other rights or licenses in respect of the Purchasing Entity.

46. Infrastructure as a Service ("IaaS")

The description of the IaaS services available under this Master Agreement, including the applicable SLA's are set out in Exhibit 5 (Cloud Cover Services) and Exhibit 6 (Cloud Platform Services) and incorporated herein.

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, Service Descriptions, 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, to the extent applicable, 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 Purchasing Entity 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 of Purchasing Entity shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, Purchasing Entity 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 Descriptions, or otherwise made a part of the Master Agreement.

> d. Unless otherwise stipulated in Section 2c, the Purchasing Entity 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 may be identified in the Statement of Work.

> e. At no time shall any Data that belongs to 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 or Statement of Work, and in accordance with applicable Data Breach laws.

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 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 Services 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.   The Purchasing Entity shall provide to Contractor a list of the primary and alternate contacts.

> b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours, or as otherwise agreed to between Contractor and Purchasing Entity, 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. If a Purchasing Entity retained Contractor to encrypt data in accordance with a Statement of Work and a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data, , 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 to the extent required by applicable state (or federal) law or as otherwise agreed to in a Statement of Work; (4) a website or a toll-free number and call center for affected individuals to the extent required by federal and applicable 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.**

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating Addendum, Statement of Work 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 the Master 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, for the fees or at the rates as agreed to in a Statement of Work, unless a unique data retrieval arrangement has been established by the Purchasing Entity and Contractor.

e. Upon termination of the Services or the Master 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 in accordance with Contractor's standard procedures, unless stipulated otherwise by the Purchasing Entity and agreed to by the Contractor. Contractor shall use reasonable commercial efforts to ensure that 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 in accordance with recognized industry practice. 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 Statement of Work.

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) request immediate replacement of the person, or if Contractor is unable to replace such personnel 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 Statement of Work for the fees specified in the Statement of Work and as agreed to by the Contractor and the Purchasing Entity directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to by the parties or as set out in the Statement of Work, 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 reasonably 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 other logs captured within the guest operating system and, unless otherwise agreed to by the parties, encryption of Purchasing Entity Data. Specific shared responsibilities are identified within the Statement of Work.

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. Any audit shall be conducted in accordance with Section 26, Records Administration and Audit of the Master Agreement.

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

12. Change Control and Advance Notice: The Contractor shall use reasonable commercial efforts to give a minimum forty eight (48) hour advance notice (or as otherwise agreed to by the parties and included in the Statement or Work or Service Description) 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 other similar public sector users.

Except upon at least 60-days prior written notice to Purchasing Entity, 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; provided, however, a successor product may remove functionality that is no longer generally utilized by users of such services.

Contractor will use reasonable commercial efforts to notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade to the extent the Contractor reasonably expects that the update or upgrade may adversely affect Purchasing Entity's use of or access to the Service.

13. Security: As requested by a Purchasing Entity and as set out in a Statement of Work, 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 service shall be available 24/7/365 (with agreed-upon maintenance downtime or due to a Force Majeure or as otherwise agreed to by the parties), and provide service to Purchasing Entity as defined in the Service Description of the Services.

17. Subcontractor Disclosure: Upon request of a Purchasing Entity and as set out in a Statement of Work, 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 internal business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service solely in connection with the IaaS; 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 or otherwise agreed to by the parties.

Attachment B – Identification of Service Models Matrix

Offerors must complete the following form to identify the service models your firm offers under this RFP. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer, including the Categorization of Risk that you have the ability to store and secure. This document is to provide purchasing entities and eligible users a quick snap shot of the cloud solutions your firm provides.

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

Attachment C – Cost Schedule
_____

Solicitation Number CH16012
NASPO ValuePoint Cloud Solutions RFP

Cloud Solutions By Category. <u>Specify **Discount Percent %** Offered for products in each category</u>. Highest discount will apply for products referenced in detail listings for multiple categories. <u>Provide a detailed product offering for each category</u>.

Software as a Service   Discount % __N/A__

Infrastructure as a Service   Discount % __7%__

Platform as a Services   Discount % __N/A__

Value Added Services   Discount % __10%__

Additional Value Added Services:

    Maintenance Services

         Onsite Hourly Rate $ __373__
         Remote Hourly Rate $ __320__

Professional Services

- **Deployment Services**   Onsite Hourly Rate $ __366__
         Remote Hourly Rate $ __306__

- **Consulting/Advisory Services**   Onsite Hourly Rate $ __366__
         Remote Hourly Rate $ __306__

- **Architectural Design Services**   Onsite Hourly Rate $ __366__
         Remote Hourly Rate $ __306__

- **Statement of Work Services**   Onsite Hourly Rate $ __366__
         Remote Hourly Rate $ __306__

    Partner Services   Onsite Hourly Rate $ __341__
         Remote Hourly Rate $ __281__

    Training Deployment Services   Onsite Hourly Rate $ __1,166__
         Online Hourly Rate $ __333__

STATE OF UTAH

Response to NASPO ValuePoint Cloud Solutions

RFP CH16012

Cost Proposal

Prepared For:
State of Utah, Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061
ATTN: Christopher Hughes, Assistant Director
christopherhughes@utah.gov

Submitted By:
EMC Corporation
2999 Douglas Blvd. Suite 275
Roseville, CA 95661

Contractor Point of Contact Title Page

RFP CH16012 | March 10, 2016

State of Utah, in conjunction with NASPO ValuePoint

Cloud Solutions

EMC Contact Information for this Solicitation:

NAME	TITLE	ROLE	CONTACT INFORMATION
Pamela Kunhart	Manager, Strategic Contracts Program Office State & Local Government, Education (SLED)	Individual in charge of the SLED Strategic Contracts Office*	(916) 797-7052 Pamela.Kunhart@emc.com
Joseph F. Spaniol III	Vice President, Federal & Public Sector Contracts & Assistant General Counsel	Individual Authorized to Obligate EMC Contractually	(703) 970-5161 joe.spaniol@emc.com

*SLED Strategic Contracts Program Office Address: 2999 Douglas Blvd. Suite 275 / Roseville CA 95661

EMC Corporation:

EMC is a global leader in enabling businesses and service providers to transform their operations and deliver IT as a Service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments to store, manage, protect, and analyze their most valuable asset – information – in a more agile, trusted, and cost effective way.

Table of Contents

Table of Contents

SECTION 9 – COST PROPOSAL

9.1 (M) Cost Proposal

Given that technology products generally depreciate over time and go through typical product lifecycles, it is more favorable for Purchasing Entities to have the Master Agreement be based on minimum discounts off the Offeror's' commercially published pricelists versus fixed pricing. In addition, Offerors will have the ability to update and refresh their respective price books, as long as the agreed-upon discounts are fixed. 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.

Offeror must identify its cost proposal, Attachment G, as "Cost Proposal – CH16012 Cloud solutions". No specific format is required for an Offeror's price schedule; however the Offeror must provide and list a discount from its pricing catalog. New discount levels may be offered for new services that become available during the term of the Master Agreement, as allowed by the Lead State.

Pricing catalogs should include the price structures of the cloud solutions models and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing must be all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

The Lead State understands that each Offeror may have its own pricing models and schedules for the Services described in the RFP. It is the intent to of the RFP to allow price schedules that are viewed in the traditional line item structure or price schedule that have pay-as-you-go characteristics.

An Offeror's price catalog should be clear and readable. Participating Entities, in reviewing an Offeror's Master Agreement, will take into account the discount offered by the Offeror along with the transparent, publicly available, up-to-date pricing and tools that will allow customers to evaluate their pricing.

Individual Participating Addendums will use the cost proposals pricing as a base and may negotiate an adjusted rate.

Offeror's price catalog should be broken into category for each service category. For example if an Offeror provides a SaaS offering then its price catalog should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Some Participating Entities may desire to use an Offeror for other related application modifications to optimize or deploy cloud solutions applications. Responses to the RFP must include hourly rates by job specialty for use by Participating Entities for these types of database/application administration, systems engineering & configuration services and consulting throughout the contract period. The hourly rates should be a fully burdened rate that includes labor, overhead, and any other costs related to the service. The specific rate (within a range) charged for each proposed contracted service would be the lowest rate shown unless justified in writing and approved by the Lead State. Any of these valued-added services must be included in your cost proposal, e.g., by an hourly rate.

EMC Response: EMC offers the prices in this section for Virtustream IaaS. We have provided an MSRP and discount off MSRP for this proposal.

The hourly rates on Attachment G are List Price Hourly Rates and the Net Price would be calculated by applying the discount percentage.

The Remote Hourly Rates are rates not requiring travel. The Onsite Hourly Rates are rates including travel & expenses.

EMC has provided Attachment G as a separate attachment titled "EMC - Attachment_G- Cost Proposal – CH16012 Cloud Solutions.pdf". Additionally, EMC is providing a detailed product offering for the IaaS category that we are responding to. This document has been provided as a separate attachment titled "Virtustream IaaS Price List 2016-03.xlsx".

EMC²®
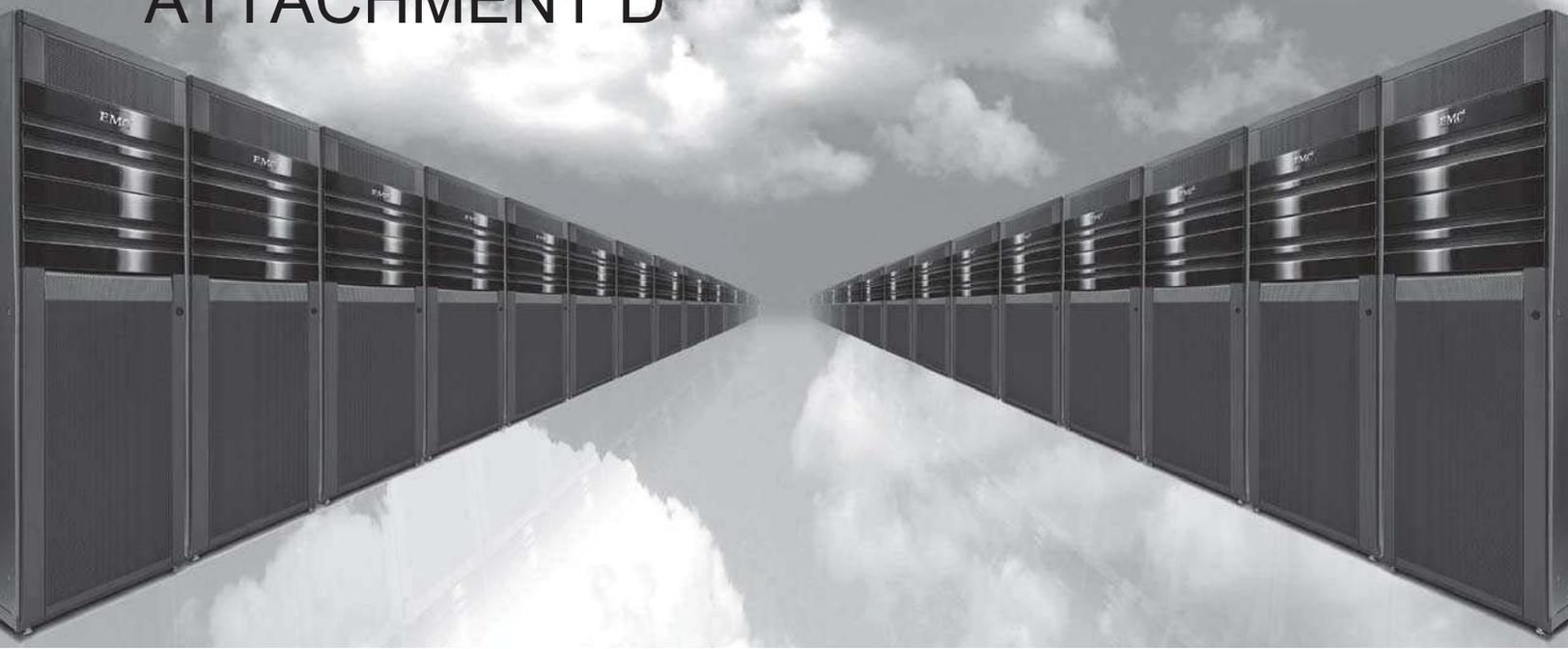
STATE OF UTAH

Response to NASPO ValuePoint Cloud Solutions

RFP CH16012

Technical Proposal

Prepared For:
State of Utah, Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061
ATTN: Christopher Hughes, Assistant Director
christopherhughes@utah.gov

Submitted By:
EMC Corporation
2999 Douglas Blvd. Suite 275
Roseville, CA 95661

Contractor Point of Contact Title Page

RFP CH16012 | March 10, 2016

State of Utah, in conjunction with NASPO ValuePoint

Cloud Solutions

EMC Contact Information for this Solicitation:

NAME	TITLE	ROLE	CONTACT INFORMATION
Pamela Kunhart	Manager, Strategic Contracts Program Office State & Local Government, Education (SLED)	Individual in charge of the SLED Strategic Contracts Office*	(916) 797-7052 Pamela.Kunhart@emc.com
Joseph F. Spaniol III	Vice President, Federal & Public Sector Contracts & Assistant General Counsel	Individual Authorized to Obligate EMC Contractually	(703) 970-5161 joe.spaniol@emc.com

*SLED Strategic Contracts Program Office Address: 2999 Douglas Blvd. Suite 275 / Roseville CA 95661

EMC Corporation:

EMC is a global leader in enabling businesses and service providers to transform their operations and deliver IT as a Service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments to store, manage, protect, and analyze their most valuable asset – information – in a more agile, trusted, and cost effective way.

EMC²

EMC²

March 8, 2016

State of Utah, Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061
ATTN: Christopher Hughes, Assistant Director
christopherhughes@utah.gov

Reference: NASPO ValuePoint Cloud Solutions RFP CH16012

Dear Mr. Hughes,

In response to the referenced solicitation, EMC Corporation ("EMC") is enclosing our proposal for the NASPO ValuePoint Cloud Solutions RFP CH16012.

EMC counts public sector entities across the United States, Europe and Asia among its most valuable customers. As a long-term partner to the public sector globally, EMC understands the mission and unique needs of the public sector. Related to the enclosed response we offer the following statements as per Section 5.2 of the RFP:

1. **As per 5.2.1**: EMC understands and acknowledges that there may be a need to negotiate additional terms and conditions, including administrative fees, with Participating Entities (PEs) when executing a Participating Addendum (PA).

2. **As per 5.2.2**: EMC staff from the EMC Corporation was responsible for writing our proposal response.

3. **As per 5.2.3**: EMC is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

4. **As per 5.2.4**: EMC understands and acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

5. **As per 5.2.5**: EMC is submitting our response to the RFP for the IaaS service model at this time. In the future, as allowed by the RFP, EMC may propose and offer additional service and/or deployment models.

6. **As per 5.2.6**: EMC is capable of storing and securing data, as defined in Attachment D at the low, moderate and high risk data categories. EMC will work with Participating Entities during the PA negotiation to make sure the risk categories for each entity are identified in advance and appropriately accommodated in each PA. As per Attachment H, EMC is able to provide deployment models for all listed in the Attachment (private, community, public and hybrid).

EMC has over 35 years of experience serving the public sector and our value is in offering solutions that help make sure that information is managed efficiently, effectively, and securely. With over 35 years in business EMC has expanded and grown to adopt to the many changes in technology. The most recent disrupting technology is less about tools and product but more about how information technology services are provided. The NASPO ValuePoint Cloud solicitation will allow public sector entities to leverage the most recent method for delivering services to constituents. EMC is proud to submit our response and help public sector customers maximize value and choice.

EMC is a Federation of companies. For this bid we are proposing on the IaaS model that is offered through our wholly-owned subsidiary Virtustream as that is our primary core competency today. Our IaaS offerings have been adopted by public and private sector organizations and will offer to Participating Entities a strong set of choices and capabilities able to scale up or down to meet constituent needs. If additional information is required, please contact Pamela Kunhart, Manager of the Strategic Contracts Program Office for EMC State & Local Government, Education (SLED). Pamela can be reached at (916) 797-7052 or pamela.kunhart@emc.com. Thank you for your consideration of our proposal.

Sincerely,

Joseph F. Spaniol, III
VP, Federal & Public Sector Contracts
EMC Corporation
(703) 970-5161
joe.spaniol@emc.com

Table of Contents

List of Figures

List of Tables

SECTION 1 – RFP SIGNATURE PAGE

5.1 (M) SIGNATURE PAGE

*Proposals must be submitted with a vendor information form, located on Bidsync as an attachment to the RFP, which must contain an **ORIGINAL HANDWRITTEN** signature executed in **INK** OR **AN ELECTRONIC SIGNATURE**, and be returned with the Offeror's proposal.*

EMC Response: EMC has provided the RFP Signature Page an attachment to the technical proposal titled "Signature Page.pdf".

SECTION 1 – RFP SIGNATURE PAGE

EMC²

SECTION 2 – EXECUTIVE SUMMARY

5.4 (M) Executive Summary

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

Our Understanding of Your Situation

The Cloud is one of the most transformative forces impacting virtually all public and private sector organizations globally. For the public sector, the cloud computing model surfaces challenges different than those in the private sector. Public sector entities have a special responsibility to protect the public trust thus it is vital that any cloud offering be thoroughly vetted to make sure the responsibilities are protected appropriately. There are several advantages the cloud model offers the public sector including:

- **Flexibility** – the cloud offers fast/quick/easy start up and shut down for small information technology needs. For example, a small test/development environment can be stood up; work performed and then shut down.
- **Transportability** – the cloud enables users to migrate from one cloud provider to another seamlessly and rapidly based on either cost, reliability or other factors. A well designed cloud offering enables this factor.

This new paradigm, in our view, can be simplified down to one thing: choice. The cloud allows public sector entities to consider different methods to deliver services to internal users and citizens. Based on the regulatory environment, on-premise, off-premise or hybrid models can be leveraged thus affording choice. For our response, we offer to Participating Entities a robust IaaS capability that we believe fits the needs of the public sector while helping make sure the public trust is secured. In the following sub section, we provide a summary description of our offering.

Our Proposed Offering

EMC is proud to offer our Virtustream IaaS solution for future use by Participating Entities. Our offering leverages the most modern technology, techniques and best quality services resources available in the market today. IaaS serves as the backbone to help organizations manage complex environments and workloads and offer a different cost structure with more flexibility for adaptors.

The most important aspect of our solution offer is choice. Participating Entities will be empowered to use move and leverage our IaaS model quickly, easily and cost effectively based on the specific short or long-term needs of their constituents. Our IaaS offer is based on the offerings of Virtustream, a wholly owned subsidiary of EMC.

Benefits of Our Solution
- **Flexible**
- **Secure**
- **Easy to Use**
- **Scalable**
- **Proven**

EMC offers several advantages with our IaaS that will benefit the Participating Entities greatly over time. First, our solution enables quick and secured provisioning providing organizations rapid utilization of an IaaS environment for short or long-term needs. Customers can leverage

our offer, integrate with others and move workloads as needed safely and securely. Second, our offer utilizes technologies that help reduce costs for customers and increase SLA metrics. Finally, EMC is SLED friendly. We have a large investment in State, Local and Educational entities and welcome the opportunity to help public sector organizations rationally adopt cloud service models and maximize value to their constituents.

Technical Approach

Our Enterprise-Class Cloud is based on being an "Enterprise Community Cloud" for multiple organizations, Federal Entities or State Agencies that require a high level of performance, security, compliance, and operational excellence. Our offer presents a private, dedicated resource pool within the larger Virtustream enterprise cloud, equipped to meet the performance, security, and SLA requirements for Participating Entities' applications. The Enterprise-Class Cloud provides Participating Entities with the benefits of a dedicated infrastructure model without the premium that is associated with it. Virtustream's product, xStream, has been developed over the course of the past 6 years with core Enterprise principles in mind: security, scalability, guaranteed performance, continuous operations, and true consumption.

Our offer supports the evolution to Cloud Computing services and EMC's wholly-owned subsidiary Virtustream, will be providing the IaaS-based security, application layer performance guarantee and multi-tenant cloud. Our offer meets the NIST definition of cloud capabilities described in Attachment D of the RFP.

VIRTUSTREAM μVM TECHNOLOGY

A key advantage of our IaaS offer is the micro-VM (μVM) technology we developed. With this unique intellectual property (IP) we are able to provide IaaS services for thousands of users around the world across six global nodes. The majority of our customers run mission-critical production applications in addition to test, development and quality assurance environments. Our μVM technology is proven to scale up and down thus providing Participating Entities the flexibility we expect they will seek when considering cloud services under the NASPO Cloud contract.

The μVM is the DNA at the heart of our IaaS offering as it is the fundamental building block of our IaaS solution. The μVM combines compute and memory, and makes sure that storage and network needs are fully provisioned. In addition our μVMs can be combined to form the optimal virtual machine (VM) for each individual application – enabling application resources to dynamically increase or decrease thus enabling Participating Entities to be assured SLA's are met without interruption. Our μVM technology works with industry standards and most common virtualization software (like VMware, Red Hat, IBM PowerVM, CentOS, and XenServer) therefore Participating Entities will have the highest degree of choice and flexibility as the consider cloud services.

The μVM brings significant benefits: enabling application level performance SLAs – which the average VM cannot normally meet. Our μVMs eliminate wasted headroom in fixed size VMs, generating significant efficiency improvements (up to 40% beyond traditional virtualization) and since our solution only charges by the μVM so you only pay for the resources you actually consume not what you might need, this typically results in lower costs to the end users. Using μVMs also enables applications to be used across multiple hypervisors, across multiple clouds

and between different locations – enabling true hybrid clouds or great choice for Participating Entities.

Summary

EMC's IaaS, created by Virtustream, is the best partner for Participating Entities seeking choice as our offer is able to meet the objectives of the RFP and enable a flexible, reliable and best-value IaaS offering. Our business is based on our ability to help our customers leverage cloud tools to help them better serve their constituents and we are committed to working with Participating Entities to make sure they get the best IaaS solution for their investment.

SECTION 3 – MANDATORY MINIMUMS

If applicable to an Offerors offering, an Offeror must provide a point by point responses to each mandatory minimum requirement. If a mandatory minimum requirement is not applicable to an Offeror's offering then the Offeror must explain why the mandatory minimum 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.

Cover Letter

5.2 (M) Cover Letter

Proposals must include a cover letter on official letterhead of the Offeror. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed. In addition, the cover letter must include:

5.2.1 A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

5.2.2 A statement naming the firms and/or staff responsible for writing the proposal.

5.2.3 A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

5.2.4 A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

5.2.5 A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.

5.2.6 A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.

EMC Response: Please refer to the Cover Letter at the beginning of this proposal.

Acknowledgement of Amendments

5.3 (M) ACKNOWLEDGEMENT OF AMENDMENTS

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.

EMC Response: EMC has provided the Acknowledgement of Amendments attachments to the technical proposal titled "EMC - ACKNOWLEDGEMENT_OF_AMENDMENTS_TO_RFP_final.pdf" and "EMC - ACKNOWLEDGEMENT_OF_AMENDMENTS_TO_RFP_final_-_02102016.pdf".

General Requirements

5.5 (M) GENERAL REQUIREMENTS

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

EMC Response: EMC agrees to provide a Usage Report Administrator responsible for the quarterly sales reporting described in the Master Agreement Terms and Conditions, and if applicable Participating Addendums. EMC maintains a Compliance Reporting System (CRS) for Public Sector contracts. Each transaction for a State government, Local government, or Education entity must be flagged and a contract vehicle must be identified before the order is placed. When the contract vehicle for the order is identified, the ordering system enforces the maximum pricing allowed on that contract for each item. This contract pricing enforcement is the same whether EMC places the order direct or a VAR places the order.

Each month EMC VARs authorized to sell via the NASPO ValuePoint contract are required to submit detailed usage reports to the Usage Reporting Administrator (URA), Tiffany Pabst. The URA then verifies each itemized sales transaction against the Purchase Order and the invoice and compiles a sales report to be sent, per the requirement, to NASPO ValuePoint and the appropriate Participating Entities. The system creates summary reports utilized to calculated NASPO ValuePoint fees as well as individual Participating Entity fees. The CRS has robust reporting capability and can produce detail product reports to aid NASPO ValuePoint and Participating Entities in managing the contract.

The table below identifies the primary contact responsible for providing the mandatory usage reports:

Table 1.   Primary Contact Information for Mandatory Usage Report

Name:	Tiffany Pabst
Telephone #:	(916) 797-6588
Email Address:	Tiffany.Pabst@emc.com

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

EMC Response: EMC agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading ordering instructions.

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

EMC Response: Virtustream has completed, provided and maintains the CSA STAR Registry Self-Assessment. We have provided a submitted CAIQ as an attachment to the technical proposal titled "EMC - Exhibit_1_to_Attachment_B_-_CAIQ_v3.0.1-09-16-2014-1.xlsx". In addition, this CAIQ is available publicly at the Cloud Security Alliances STAR Registry website.

EMC Response: The xStream platform provides the following benefits:

- Consumption-only charging, not allocation charging, *"pay only for what is used"*

- µVM technology drives hyper-efficient resource utilization— reducing costs approximately 60% compared to physical hosting and 30% compared with traditional virtual hosting

- Guaranteed IOPS delivering enterprise-class application level performance guarantees

- Enterprise-class Service Level Agreements (SLAs) with availability of 99.99%

- Reserve µVM for workloads that require DR capacity

- Virtually unlimited scalability IaaS; automated and on-demand via cloud portal

- Backup as a Service on xStream cloud offers restore and a charging model based on a low cost per gigabyte based on actually protected data.

- Virtustream's standards with respect to µVM s and storage:

Table 2.   Virtustream Standards for µVMs and Storage

STANDARD ATTRIBUTE	BASIC PLUS ENTERPRISE	HIGH MEMORY ENTERPRISE	RESERVE(DR)
SLA Guarantee	99.99%	99.99%	99.99%
Network Access	VPN/MPLS/P2P	VPN/MPLS/P2P	VPN/MPLS/P2P
Storage Service Level	4 Tiers, Local or Replicated	4 Tiers, Local or Replicated	Needs replicated storage
Data Resiliency Service Options	Backups – local or replicated	Backups – local or replicated	Needs Replicated Backups
Compute Memory Size	<64GB	>64GB	
Availability of Resources			
µVM	Single Site _ primary	Single Site – primary	Single Site - secondary
IOPS	Best Available	Best Available	Guaranteed/Best Available
Reservation Status	Priority	Priority	Priority

Recertification of Mandatory Minimums and Technical Specifications

EMC Response: EMC will annually certify to the Lead State that it still meets or exceeds the technical capabilities in our proposal.

SECTION 4 – BUSINESS PROFILE

Business Profile

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.

EMC Response: Founded in Newton, Massachusetts, in 1979, EMC Corporation is a global leader in enabling businesses and service providers to transform operations and deliver IT as a Service (ITaaS). EMC is focused on helping our customers lead in three of the most important areas of IT investment:

- **Big Data**: Leveraging vast quantities of data to make smarter decisions and solve complex problems
- **Trusted IT**: Protecting and securing information to ensure that IT is trusted
- **Cloud**: Improving agility and reducing IT costs through the adoption of cloud computing and IT transformation initiatives

BROAD RANGE OF CUSTOMERS

We work with organizations around the world, in every industry, in the public and private sectors, and of every size, from startups to the Fortune Global 500. Our customers include global money center banks and other leading financial services firms, manufacturers, healthcare and life sciences organizations, Internet service and telecommunications providers, airlines and transportation companies, educational institutions, and public sector agencies.

STRONG LEADERSHIP RECORD

Our differentiated value stems from our sustained and substantial investment in research and development, a cumulative investment of $20.7 billion since 2005. To strengthen our core business and extend our market to new areas, EMC has invested $16 billion in acquisitions over the same period and has integrated more than 75 technology companies.

EMC is supported by thousands of technical R&D employees around the globe, the industry's broadest portfolio of systems, software, and services, our ability to create total integrated solutions, and our commitment to delivering the best Total Customer Experience in this or any industry. In 2014, EMC customers awarded the company our highest net promoter score ever recorded, and our service excellence was recognized by distinguished awards for Innovation in Customer Commitment and Innovation in Enabling Customer Success from the Technology Services Industry Association.

We operate R&D centers in Brazil, China, France, India, Ireland, Israel, the Netherlands, Russia, Singapore, and the U.S., and manufacturing facilities in the U.S. and Ireland. We hold the most stringent quality management certification from the International Organization for Standardization (ISO 9001), and our manufacturing operations hold an MRP II Class A certification.

EMC ranks 121 in the Fortune 500 and had reported revenues of $24.7 billion in 2015, the largest revenue year in EMC's 36-year history.

GLOBAL PRESENCE

EMC employs approximately 72,000 people worldwide. EMC employee retention rates specific for employees that may be associated with the services related to the RFP over the last two (2) years are approximately 85% 2014 and 2015.

We are represented by approximately 400 sales offices and scores of partners in 86 countries around the world. We have the world's largest sales and service force focused on information infrastructure, and we work closely with a global network of technology, outsourcing, systems integration, service, and distribution partners.

We are a publicly traded company, listed on the New York Stock Exchange under the symbol EMC, and are a component of the S&P 500 Index. We are committed to acting in a socially and environmentally responsible manner and to being an attentive and thoughtful neighbor in our local and global communities.

Figure 1.   EMC Global Presence

EMC EXECUTIVE AND SENIOR MANAGEMENT

Table 3.   EMC Executive Team

Name	Title
Joseph M. Tucci	Chairman and Chief Executive Officer
William J. Teuber, Jr.	Vice Chairman
David I. Goulden	CEO, EMC Information Infrastructure
Howard D. Elias	President and Chief Operating Officer, Global Enterprise Services
Jeremy Burton	President, Products and Marketing
Bill Scannell	President, Global Sales and Customer Operations
Paul T. Dacier	Executive Vice President and General Counsel
Erin McSweeney	Global Human Resources
Zane Rowe	Executive Vice President and Chief Financial Officer
Rodney Rogers	CEO, Virtustream

Table 4.   EMC Business Executives

Name	Title
Guy Churchward	President, Core Technologies Division, EMC Corporation
Chirantan "C.J." Desai	President, Emerging Technologies Division
Rohit Ghai	President of the Enterprise Content Division
John Roese	Senior Vice President and Chief Technology Officer
Chad Sakac	President of EMC's Converged Platforms Division, VCE
Amit Yoran	President, RSA, The Security Division of EMC
Kevin Roche	President, EMC Global Services
Chris Riley	Senior Vice President, Americas Enterprise Sales, EMC
Adrian McDonald	President, Europe, Middle East and Africa
David Webster	President, Asia Pacific and Japan Senior Vice President
ML (Mary Louise) Krakauer	Executive Vice President, Enterprise Business Solutions and Chief Information Officer, EMC
Nina Hargus	Senior Vice President, Chief Marketing Officer EMC Corporation
Irina Simmons	Senior Vice President and Chief Risk Officer
Harry L. You	Executive Vice President
Kevin Reid	President and Chief Technology Officer, Virtustream

EMC PUBLIC SECTOR

EMC helps a wide range of public sector organizations—local and national, small and large, around the world—transform government with innovative information infrastructure services and technology.

EMC helps customers leverage information assets, improve interfaces with constituencies, increase operational efficiency, reduce costs, ensure data security and regulatory compliance, and strengthen functional capabilities. Some of the public sector solutions we offer include:

- **Defense, Civilian and Intelligence Solutions** - Leverage EMC's information storage and management systems to deploy solutions that can be configured to meet requirements for the highest government levels for security, reliability, and scalability.
- **Education Solutions** - Leverage affordable and effective information management capabilities for colleges, universities, K-12 education, e-Learning, students, faculty, and research institutions.
- **Public Health Solutions** - Deliver public health services in a timely, efficient, and cost-effective manner—serving more citizens despite increasingly complex delivery systems.
- **Public Safety and Justice Solutions** - Integrate, modernize, and automate your operations to improve citizen services. Respond quickly to any information-related public safety or judicial challenge.
- **Revenue, Finance, and Taxation Solutions** - Protect and share financial data, and optimize the design and implementation of your organization's tax, treasury, assessor, and other finance systems.
- **Social/Human Services and Benefits Solutions** - Deliver high-quality and citizen-based responsiveness in a cost-effective manner. Consolidate, modernize, and streamline important functions to effectively transform your IT infrastructure.
- **Transportation, Planning, and the Environment Solutions** - Establish and enforce clear policies and efficient processes for addressing data-intensive challenges related to transportation systems, government planning requirements, and environmental management.

EXPERIENCE PROVIDING CLOUD SOLUTIONS

Cloud computing, delivered by EMC's wholly owned entity Virtustream, has been hailed as a solution to these challenges offering improved efficiency and scale, and enabling dynamic on-demand IT. However few cloud offerings today are able to meet the stringent requirements of enterprise customers, including:

Cloud computing, delivered by Virtustream, has been hailed as a solution to these challenges offering improved efficiency and scale, and enabling dynamic on-demand IT. However few cloud offerings today are able to meet the stringent requirements of enterprise customers, including:

- Enterprise Grade Security & Compliance

- Application Performance SLAs & Assurance

- Consumption-based Pricing & Chargeback

- Legacy Application Support

- Hybrid Support for On & Off-site Control

Virtustream is one of the few providers today who has developed industry leading IP and, from it, built an enterprise cloud platform. Our platform already serves thousands of users around the world across six global nodes. The majority of these users are running production mission-critical application environments in the cloud alongside Test & Development environments that support them. We also understand that applications behave differently in a cloud environment and we are one of the few providers able to optimize applications so that they are at peak performance when running in the cloud.

µVM Technology

Our platform is designed and built with µVM™ technology. The µVM is the DNA at the heart of the cloud, the fundamental building block of cloud operations. The µVM combines compute and memory, and assures storage and network. µVMs can be dynamically combined to form the optimal virtual machine (VM) for each individual application – enabling application resources to dynamically increase or decrease. µVMs are the fundamental unit of measure within a cloud, and between clouds and is designed to work among and between other virtualization products (like VMware, Red Hat, OpenStack, CentOS, and XenServer) thus enabling more choice for Participating Entities.

The µVM brings significant benefits such as enabling application level performance SLAs – which an average virtual machine cannot. µVMs eliminate wasted headroom in fixed size VMs, generating significant efficiency improvements (up to 40% beyond traditional virtualization) and customer are only charges by the µVM so you only pay for the resources you actually consume not what you might need, thus reducing cost to Participating Entities vs. other market offerings. Using µVMs also enables applications to be used across multiple hypervisors, across multiple clouds and between different locations – enabling true hybrid clouds. µVM technology allows EMC² to offer enterprise class clouds capable of running both mission-critical enterprise applications and web-scale applications, delivering the full benefits of cloud to the enterprise.

Experience Providing Cloud Solutions For Government Projects

The following offers a summary of experience with providing cloud solutions for government projects:

Table 5. **Summary of Experience with Department of Transportation**

Name of Customer:	Department of Transportation
Contract/Project Number:	Department of Transportation: Commercial Driver's License Gateway
Contract Type:	Fixed Price, 5 Year Term
Description of the Work Performed:	The FMCSA CDLIS Gateway is enterprise grade software and services Infrastructure on a Service platform. The major component of the FMCSA Gateway is the secure high-performance platform that orchestrates virtual machines using VMWare hypervisors.

The Federal Motor Carrier Safety Administration (FMCSA) is an Operating Administration within the U.S. Department of Transportation (DOT) with a mission to reduce commercial motor vehicle-related crashes and fatalities. In part, FMCSA's stakeholders and business processes are supported through a suite of Legacy Information Technology (IT) systems, of which the majority reside within the VOLPE data center and are made accessible through the FMCSA web portal (hereinafter Portal). Additionally, there are systems outside the FMCSA Portal, which are operated independently; of which four (4) such systems are the Commercial Driver's License Information System (CDLIS), the National Law Enforcement Telecommunications System (NLETS), Mexico's motor carrier authorization database, the commercial driver's licensing system (eLicencias), and the Federal Convictions and Withdrawals Database (FCWD).

Under a cooperative exchange of commercial driver information between the CDLIS jurisdictions (i.e., the United States, Mexico, and Canada) the systems form a Gateway to information and are largely a database with source information received from groups such as American Association of Motor Vehicle Administrators (AAMVA), the government of Mexico and of Canada, and others. In turn, the collective information is used in national compliance reviews by the Commercial Driver's License (CDL) Division supporting the North American Borders Division with safety systems and program projects; federal and state jurisdictions in the United States; State and Local governments; and is used by corresponding jurisdictions in Canada and Mexico.

FMCSA relies on the Gateway to support a number of electronic transactions for CDL/Carrier/CMV inquiries (approximately 5 million annually), and Federal Convictions and Withdrawals Database (FCWD) requests (approximately 10,000 annually) and has 13,000 users.

The system was awarded an ATO in April 2013 and was recently audited to NIST 800-53r4 successfully in April 2014. All System Security Plans and attachments are in place and reviewable by authorized (By DOT) US Government Agencies. An ATO is currently in process. |
| Period of Performance: | Sept 2012 – Present (ATO is renewed in April yearly.) |
| Competitive Advantage: | Virtustream's Federal Cloud offers the advantages of a fully managed, high performance, highly secure, FISMA-certified infrastructure. In addition to the technical advantages versus other commodity cloud service, this project supports the Federal Data Center Consolidation Initiative encouraging all government organizations to embrace cloud computing in order to reduce data center footprint. |

Table 6.   Summary of Experience with Department of Interior

Name of Customer:	Department of the Interior
Contract/Project Number:	Department of the Interior: Financial Business Management Systems
Contract Type:	Fixed Price
Description of the Work Performed:	Virtustream, a leading enterprise class cloud software and Infrastructure-as-a-Service (IaaS) provider is working with prime contractor Unisys to migrate the U.S. Department of the Interior (DOI) Financial and Business Management System (FBMS) to the cloud. Unisys was recently awarded the first task order under the DOI Foundation Cloud Hosting Services (FCHS) indefinite delivery-indefinite quantity (IDIQ) contracts. As a subcontractor to Unisys, Virtustream will host FBMS, on its high-performance, federal enterprise class IaaS cloud.
	With multiple locations and a complex IT environment, DOI needed to move to a highly efficient virtual environment hosted in the cloud. Virtustream's enterprise class IaaS cloud, powered by its xStream cloud management software and µVM™ technology, provides the necessary capabilities to meet the DOI's business, security and reliability requirements. Virtustream is SAP-certified in both cloud and hosting services and has extensive experience in migrating enterprise mission-critical applications to the cloud. Virtustream also possesses a Virginia-based data center that is FISMA-certified, which is essential for federal compliance requirements.
	The system was granted a P-ATO in January 2014 and a full ATO is expected to be granted in June 2014.
	Note: This project is hosted in the Virtustream Federal Cloud (IAAS) that is currently undergoing GSA FedRAMP Compliance. Expected Provisional Authority to Operate (P-ATO) is expected in in September 2014.
Period of Performance:	May 2013 – Present (ATO granted in April 2014)
Competitive Advantage:	Virtustream is providing infrastructure as a service for the Department of Interior in a secure and compliant infrastructure that allows DOI's infrastructure to grow as their business requires. The DOI project needs to be delivered in a FedRAMP audited cloud, and protect sensitive data with FISMA-Mod controls. DOI required disaster recovery and high availability embedded in their solution. Virtustream's infrastructure as a service allows customers to select a pre-architecture infrastructure model that includes disaster recovery as an embedded option.

Scope of Experience

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.*

EMC Response: The following represents our experience with government or large consortium contracts similar to the Master Agreements sought through this RFP.

US DEPARTMENT OF INTERIOR

The U.S. Department of the Interior (DOI) is comprised of 70,500 employees in 2,400 locations across 12 time zones and manages more than 500 million acres (about 20%) of the land area of the United States. The Department is responsible for the 401 properties in the national park system, 556 national wildlife refuges, 71 fish hatcheries and one historic fish hatchery, 21 national conservation areas, and 16 national monuments. The DOI has a significant information technology footprint. Currently the 13th largest Federal civilian agency in terms of IT spending, the DOI has an IT budget of just over $1 billion.

DOI is undergoing a decade-long transformation of its IT systems, moving away from government-owned data centers and towards a cloud computing model. The first system the DOI has chosen to migrate to the cloud is a mission-critical application called the Financial and Business Management System (FBMS) which is based on SAP's enterprise resource planning (ERP) software platform. FBMS has over 20,000 users and incorporates Finance, Acquisition, Financial Assistance, Personal Property, Fleet, Real Property, and Enterprise Management Information System (EMIS) functionality.

Moving FBMS to the cloud allows DOI to begin the process of closing or consolidating potentially hundreds of DOI data center allowing the agency to reduce overall operating and maintenance costs while enabling a new generation of innovative services. Prime contractor Unisys partnered with Virtustream to migrate FBMS to Virtustream's secure, high-performance, FedRAMP certified cloud environment.

A project team consisting of SAP-certified migration specialists moved FBMS onto the x86-based Virtustream cloud. Virtustream's xStream-powered Enterprise Class Cloud provides the DOI with a flexible, cost-effective, high availability cloud platform, offering the agency a 99.999% uptime SLA for all workloads.

As a Federal agency, security is a critical consideration for the DOI. Virtustream's data centers have received FISMA moderate authority to operate (ATO) and are FedRAMP certified. Furthermore, the Virtustream cloud is architected to support the industry's highest security and compliance standards, including SSAE 16, PCI, DIACAP, G-Cloud, Shared Assessments, ISO27001, ITIL v3.0 and more.

The DOI's SAP migration is one of the first mission-critical Federal applications to be migrated to the cloud and is now in full production in the Virtustream Federal Cloud. DOI expects to save roughly $100 million in infrastructure and IT costs each year from 2016 to 2020 by migrating to the Virtustream Cloud. Along with the financial impact of its migration, the agency will realize significant additional benefits, including: increased reliability, greater and more predictable application performance, greater visibility into system cost and performance, greater compliance through improved security and internal controls, and faster and easier system updates.

The approximate dollar value for this contract was $36,000,000.

DEPARTMENT OF VETERANS AFFAIRS

The Department of Veterans Affairs (VA) implemented the Veterans Health Information Systems and Technology Architecture (VistA) which is the VA Electronic Health Record (EHR). The Medical Appointment Scheduling System (MASS) is a scheduled enhancement to VistA to replace the current scheduling system which has failed and drawn a great deal of negative attention to the VA. The MASS project will replace the current inpatient and outpatient

scheduling system which was built in the early 1980's as an inpatient care scheduling system with few embedded business rules. In fiscal year (FY) 2013 approximately 8.9 million of the 21.9 million living Veterans in the nation were enrolled in the VA health care system. VHA's 50,000 users scheduled over 100 million appointments in FY2014 for this Veteran population.

Solicitation is a single award IDIQ- 5yr base, 2 option yrs. Task Orders will be issued to gradually deploy the replacement MASS. There are no Day 1 Task Orders included in the solicitation. VA requires a commercially available off-the-shelf (COTS) based medical appointment scheduling solution that incrementally improves scheduling as it is integrated with VistA and deployed across the enterprise.

The U.S. Department of Veterans Affairs (VA) was under pressure from congress to decrease veteran wait times and replace their 25-year-old scheduling software - VistA. VistA currently schedules a patient with a doctor, whereas most commercial systems schedule all clinical resources including medical equipment and facilities necessary for care. This prevents the VA from being able to optimize resource utilization. The VA needed to replace the current scheduling system with one that provided full resource scheduling capabilities, ease of use to the medical schedulers in the VA network and provide a self-service portal functionality to the veteran.

The challenge was to provide a world class scheduling system, upgrade the current system while maintaining current service levels, and complete this effort quickly and under a tight and highly scrutinized budget. The VAMASS EPIC implementation will represent the VA's largest mission critical application hosted in an off premise cloud environment. The VA will have a modern, feature rich and secure scheduling system utilizing EPIC and the Virtustream IaaS (Infrastructure as a Service) platform.

EMC's Virtustream is providing a stable secure infrastructure at an overall cost saving to the project utilizing our xStream cloud management software. Our solution also continuously monitors and provides reports to meet Government reporting requirements using our Viewtrust software (this was a critical piece in the VA's selection process). The EPIC/Virtustream solution will give the VA a highly available and user friendly system that will enable the VA schedulers to schedule nationwide on a single system. The EPIC/Virtustream solution will provide clinical resource tracking and reporting, enabling the VA to manage resource availability, leading to higher resource utilization and shorter wait times for veterans.

The approximate dollar value for this contract was $70,000,000.

UOL GROUP

UOL Group is the leading internet services company in Brazil. The company was founded in 1996 as a content and services portal, and has expanded to become the second largest media conglomerate in the country. The UOL portal is ranked among the top 100 most visited websites in the world. In addition, the company provides internet access in more than 3,000 cities throughout Brazil. UOL Cloud is an entity within UOL Group formed in 2014 by the combination of UOL Host, a hosting and web services company targeting small and medium sized businesses (SMBs), and UOL Diveo, Brazil's largest IT data and infrastructure provider, targeting the enterprise.

UOL Cloud has four data centers in Brazil, the newest of which, Data Center UOL, is among the largest in the world, hosting over 16,000 servers and 9 PB of storage capacity. UOL Cloud has a

portfolio of more than 3,000 corporate clients, offering them a wide range of data center, telecommunications and integrated IT services. With a reputation for innovation, UOL was in a unique position to serve the rapidly expanding market for cloud computing services in Brazil, estimated to be grown at greater than 70% per year over the next three years by analyst firm IDC. Recognizing the opportunity ahead of it, UOL set out to become the number one provider of cloud services in Brazil.

To achieve its goal, UOL knew it couldn't offer only commodity-grade cloud computing services to SMB customers. Rather, it would need an offering capable of meeting the cloud computing needs of its tough-to please enterprise customers. A key challenge UOL faced: To get there quickly. With plenty of regional and global competition, UOL couldn't afford missteps. The company needed a proven way to quickly field an enterprise-ready cloud computing service. After careful evaluation, UOL selected our xStream cloud management software to expand its portfolio.

xStream allows the company to offer the secure, reliable, high-performance cloud computing solutions its enterprise clients demanded. With xStream, UOL is able to migrate its customers' mission-critical applications to the cloud, while providing application performance SLAs, multi-tenant efficiency, and a consumption-based pricing model for both legacy (SAP, Oracle, Microsoft, etc.) and modern web-scale applications. To ensure high levels of operational efficiency, UOL will transition its existing public cloud offering to xStream, allowing it to consolidate its cloud platform and infrastructure and manage both through a common interface.

In addition to providing the xStream software, UOL engaged our advisory services to rapidly achieve the goals of its business model and go-to-market strategy for the enterprise market. As a result UOL met its aggressive deployment timeline. From a cold start, the company launched a full-featured enterprise-grade cloud computing offering in less than three months. UOL's cloud quickly delivered promised benefits to the company and its customers.

UOL previously required ten days to bring a customer's first server on-line, customers can now be provisioned in the cloud in two days or less. And once on board, users can launch new servers in seconds via a self-service portal. Said UOL, "Virtustream's software offers the features and capabilities we need to ensure our enterprise customers are able to move their business-critical applications to the cloud, without concerns over security and compliance, performance or cost. Our cloud service portfolio, in conjunction with Virtustream's xStream, will set the bar for the cloud market in Brazil." UOL is so confident in their new cloud that they've committed to transition their own estate of over 30,000 servers to the cloud. No stranger to aggressive timelines, the company expects to migrate 70% of its IT landscape to the cloud within the next two years.

The approximate dollar value for this contract was $7,649,438.

DOMINO SUGAR

Cloud Domino Sugar, part of American Sugar Holdings, is the largest manufacturer and distributor of sweetener products in North America, inclusive of the Domino®, C&H®, Redpath® and Florida Crystals® brands. The company has grown to become a multi-billion dollar enterprise, producing four million tons of sugar per year with 180,000 acres of growing land, mills, distribution centers and an energy facility. There's no question that Domino Sugar views IT as a critical part of business, offering competencies to improve overall operations. As

such, it is vital that they leverage best-of-breed infrastructure to ensure that their IT operations run efficiently, costs are controlled, and data is secure. Considering the proven benefits the cloud offers enterprises, Domino investigated the prospect of moving all of their IT infrastructure to the cloud to enhance IT operations, reduce risk and offload IT management, thereby redirecting IT resources to focus on other strategic projects and business process improvements.

Global Business Operations Challenges and the IT Environment Domino markets and distributes products into three primary distribution channels: Industrial, Consumer (selling the three leading sugar brands in the United States), and Foodservice. All channels include a component that is export related and they continue to expand their international presence through acquisition. In 2010, their parent company American Sugar Refining Inc. completed its acquisition of Tate & Lyle PLC's European sugar refining business. Offering commodity products on a global scale presents various IT challenges associated with integrating operations. With several businesses operating in multiple countries around the world and new systems being added regularly, Domino's IT infrastructure is incredibly complex and has gone through many migrations. Their IT environment began as a traditional on-premise data center. To optimize their operations over the years, however, they've eliminated as much hardware as possible and turned to vendors to house their software and data offsite. They moved first to a co-located environment, then to a hosted environment, and finally to an application services contract. They have also historically tested and implemented new enterprise technologies and delivery methods to improve IT operations.

For instance, they were early adopters of application outsourcing for their SAP deployment, which has grown in size and complexity. All critical production systems are driven by SAP, including enterprise resource planning, customer relationship management, invoice and orders systems, business intelligence, human capital management and payroll, among others. Defining Goals and Identifying Trusted Partners Though Domino Sugar continues to grow and expand operations; the IT team has managed to maintain their IT budget at less than one percent of overall revenue. For ongoing efficient management of their IT infrastructure, they looked to the cloud to deliver flexibility and cost savings while improving speed, reliability and security of SAP production systems.

They remained firm that whatever deployment option they chose could not sacrifice - even in the slightest - the performance of the SAP systems, which managed over 20 TB of data for thousands of users in North America. When considering multi-tenant cloud vendors, Domino evaluated platforms based on the ability to guaranteed compute resources, data protection and industry leading SLAs. They wanted assurance that security and performance requirements were part of the contract. After evaluating several cloud platforms, Domino found the xStream platform was the only true private cloud solution running within a multi-tenanted environment that could provide the right combination of performance and security worthy of their enterprise-class requirements. Our utility billing model stood out as a strategic advantage as it offered Domino the ability to pay only for the precise computing power that they consumed. Under their previous ASP model, they were constrained by the technology as adding capacity or storage required a lengthy commitment and often led to underutilized infrastructure.

Following a 90-day migration process, Domino deployed their entire IT infrastructure on xStream, our consumption-based cloud platform capable of handling complex production applications. The project included a multi-thousand seat SAP enterprise application system. As a result, SAP systems now operate up to twice as fast on xStream and are highly available and

secure. The xStream platform leverages an Intel Xeon processor 5680, which delivers a twofold performance increase over non-virtualized, older generation Intel processor - based servers. Domino projects up to a 40 percent reduction in total cost of ownership over three years, while also increasing availability and shrinking disaster recovery times.

The cost savings enable business growth and the flexibility they gain from running applications on the cloud enables their team to focus on delivering business value rather than managing hardware. The most significant cost savings are associated with eliminating the need to purchase hardware for a specific amount of time. Our utility-based deployment and pricing gave Domino the flexibility to rapidly add resources as needed. This allows for a more efficient utilization of resources and a true consumption based pricing model. Managed services will also be purchased based on aggregate workload per month rather than by infrastructure provisioned, delivering further efficiency to the bottom line.

Usually production and non-production systems are at risk of a hardware failure causing downtime of as much as 4 hours or more. For Domino Sugar all systems are highly available with little risk of (not to) downtime due to hardware failure. Similarly in the event of a disaster, up to 24 hours of data could be lost and it would take at least two days to restore systems albeit with impaired performance. No all production systems will be mirrored to an alternative site resulting in near zero data loss and less than one hour to restore full performance.

In conclusion, with the deployment onto xStream complete, Domino effectively runs the largest SAP production environment running in a multi-tenanted private cloud. This deployment shows a shift in thinking - CIOs and other IT professionals are beginning to trust cloud platforms and understand the benefits that can be achieved from cloud deployments.

The approximate dollar value for this contract was $64,327,253.

DIESEL DIRECT

When Hurricane Irene hit Eastern Massachusetts last August, the roads were filled with broken trees and downed power lines, leaving many without power for more than a week. When Diesel Direct, a trucking and construction businesses, was affected by this power outage, its founder sought an alternate plan for keeping the business active under such circumstances. He found his answer in the cloud. Diesel Direct fuels and services trucks nationwide for clients of all sizes. Its workers--who ghost in and out of truck-fleet parking yards so early even the crack-of-dawn loaders and drivers sometimes don't see them feeding the trucks--use handheld scanners to record how much fuel and service they give each truck, then upload that data to Diesel Direct, which can then send out invoices for the work that same day.

The Challenge was that the company relied on the expertise of a staff of experienced billing agents, account managers and administrative specialists whose primary tools were one giant customer database built on Microsoft Access, Exchange email and the anachronistic but effective use of paper invoices delivered via fax or snail mail. This process was effective until Irene made it clear that if power went out in the main office Diesel Direct wouldn't be able to send out that fast flurry of invoices every day. And without that, their cash-flow situation would be greatly impacted very quickly. Fleet managers for distribution companies, understand quickly how Diesel Direct can save them money by letting them trade a few extra cents per gallon of fuel for the FTE cost of having their own people handle the fuelling and maintenance and reporting, plus

the cost. Diesel Direct decided to adopt a virtual/private cloud strategy with disaster recovery to hedge against business loss due to unexpected power outages or other unforeseen events.

Solution Diesel Direct hired Virtustream, because of the range of alternatives available in each of three categories that it needed--private, virtual private and public cloud. Diesel Direct hired Virtustream to host its data and slightly upgraded versions of its software so employees could work from the same office using the same interfaces and workflow they always had. The only difference was that the data and apps were all housed in a data center outside Washington, D.C. and replicated to another.

From an operational IT perspective, the biggest benefit of our offering is the rapid, repeatable changes in capacity that our tools allow customers. Diesel Direct's business is "bursty"--doubling or tripling from one day to the next, changing with the flow of invoices. Our service contract allows Diesel Direct to set a relatively high average baseline, and then change its top capacity demand limit as often as it wants--every day if that's what works for the customer. Adding capacity is as easy as changing a configuration screen; so is reducing capacity when the spike disappears.

Those changes save Diesel Direct both money and time. Rather than running reports and invoices all night Tuesdays, for example, the additional capacity lets the company run those resource-intensive processes during the day rather than overnight. That gets critical work done faster and more accurately than a process left to complete itself unattended. The benefits from dynamic capacity management and professional management are a perfect example of why people are going to embrace cloud computing even in $300 million non-tech-focused companies. These companies don't want to spend a lot of money on IT, don't have the budget to do best-practice on-premise infrastructure, so being able to leverage another company's resources like those we offer affords them a distinct advantage for their business.

The approximate dollar value for this contract was $336,230.

Financials

6.3 (M) Financials

Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

EMC Response: EMC has provided the audited financial statements as an attachment to the technical proposal titled "EMCCorporation_2015_10KReport.pdf".

EMC's D&B number is 09-744-7148. EMC's credit rating as of February 2, 2016 is 5A2. A copy of the D&B Report has been provided as an attachment to the technical proposal titled "EMC - Dun & Bradstreet Report - February 2016.pdf".

General Information

> ## 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.*

EMC Response: Virtustream is an innovative cloud solution provider committed to delivering next generation cloud services for enterprises. Our solution leverages our secure, high performance platform, called xStream ™, to deliver highly available and elastic compute services at true consumption-based pricing. xStream™ is our cloud management software with industry-leading features for performance management, security, compliance and native hybrid control.

We offer our clients a self-service portal called the xStream™ portal. The xStream™ platform has been designed to provide enterprise IaaS services, and specializes in moving complex enterprise IT environments to the cloud.

Our IaaS offering is the right strategic partner for Participating Entities interested in a flexible and secure IaaS requirement. The services fit squarely into our area of expertise, experience and core competency. By leveraging our comprehensive set of SLA backed Cloud Infrastructure, Application Management, Migration and Support services, based on our xStream™ cloud platform, we will be able provide Participating Entities a flexible, cost effective, highly available, highly performant solution and platform which is flexible and expandable for any future growth or new systems.

Figure 2.   Supporting Enterprise Customers

In contrast to traditional hosting solutions where fixed hardware resources must be allocated to applications, or typical public cloud offerings where performance, security and control are mostly weak, Virtustream services offer the best of both worlds by combining the scalability,

cost savings, and CAPEX to OPEX conversion inherent in public clouds with the control, security and service levels associated with dedicated hardware, hosted, or private cloud implementations. Virtustream's purpose is to support the mission critical IT requirements of Enterprise Class customers demanding SLA backed services that meet rigorous compliance, security and budgetary criteria. Virtustream's platform architecture, coupled with our patent pending μVM technology is supported by the world's leading experts in virtualization. Our holistic approach to service delivery includes world-class professional and support service teams:

Flexible, Agile and Cost Effective IT

- Virtustream's *xStream*® Cloud services are inherently flexible and scalable. Compute resources are made available on demand.

- Virtustream ensures the most cost effective solution by providing true consumption based billing. Unlike traditional hosting or public cloud services, Virtustream's patent pending μVM ™ technology can guarantee that Participating Entities only pay for compute resources that are actually used. This is a critical distinction when compared to virtual machine or host based billing methodologies.

- The μVM enables efficiencies beyond traditional Virtualization. These efficiency gains translate into improved workload management and cost reductions.

CAPEX to OPEX Conversion

- Beyond fixed migration and implementation costs, our proposal is for a highly agile and flexible OPEX model. Inherent in our solution is the ability for Participating Entities to "operationalize" costs.

Eliminate Technology Refresh Concerns

- Virtustream is responsible for delivery service per SLA. By shifting the burden of Infrastructure and support to Virtustream, Participating Entities will be able to get out of the technology refresh cycle.

Enhanced DR and Business Continuity Options

- The IaaS solution is architected with embedded DR and replication features that provide 15 minute RPO and 2 hour RTO at fraction of the costs normally associated with such a robust DR capability. The IaaS platform leverages fully redundant and meshed data centers to ensure Participating Entities have the best possible business continuity plan.

Application Performance Improvements

- Virtustream customers typically experience 20% to 100% improvement in application response times. This is achieved via tuning our system to support applications and rigorously maintaining our platform to deliver the best possible performance.

- μVM technology ensures the best possible workload management including instantaneous availability of compute resources, CPU and Memory.

- The IaaS, depending on the SLA level, can guarantees disk throughput and latencies; ensuring disk read/write is not a bottleneck to performance.

Enhanced Security

- The IaaS Platform is architected to the highest security and compliance standards enabling enterprises to follow best practice frameworks including SSAE16, PCI-DSS, FISMA, G-Cloud, FedRAMP, ISO 27001, ITIL v3.0 and other industry standards.

- The xStream Platform utilizes a defense in-depth guiding principle that is multi-tiered for all virtual and physical infrastructures and includes proactive threat monitoring.

- Virtustream has integrated Intel's Trusted Execution Technology (TXT) into the IaaS Platform. Virtustream is the first provider embedding TXT into a cloud platform.

Customer Centric and Collaborative Support Model

- The support objective is to offer world-class assistance to our clients as a partner rather than simply as a vendor. We offer a 24x7x365 service desk, fully trained and certified staff, and support options to meet all requirements and budgets.

- Virtustream will establish a defined feedback loop via regularly scheduled meetings with customers that subscribe to the IaaS and the account team.

- Participating Entities will have a high level of visibility into their environment via our *xStream®* support dashboard where real-time information regarding your landscape is available and where, should you choose to, a Participating Entity can self-manage services.

Cloud Market Considerations

- Recognized as a 2014 leader in the Gartner's Magic Quadrant for Cloud Services (IaaS), Gartner highlights Virtustream strengths to include a management team and founders that have technical and leadership backgrounds in VMware and SAP consultancies and hundreds of years of combined experience working with Enterprises.

- Virtustream's Cloud Platform powered by *xStream®* is supports mission-critical production applications supporting both traditional enterprise workloads, in addition to cloud-native applications.

- Unique approach to the market and technology with enterprise focus and µVM.

- Rated highest on Security & Compliance* >10% higher than other provider (*Gartner*).

- Overall performance/price value was >**11% higher** than any other Cloud provider and **30-50% greater** than the remaining providers in the tests. (*Cloud Spectator*).

Figure 3.   Gartner and Cloud Spectator
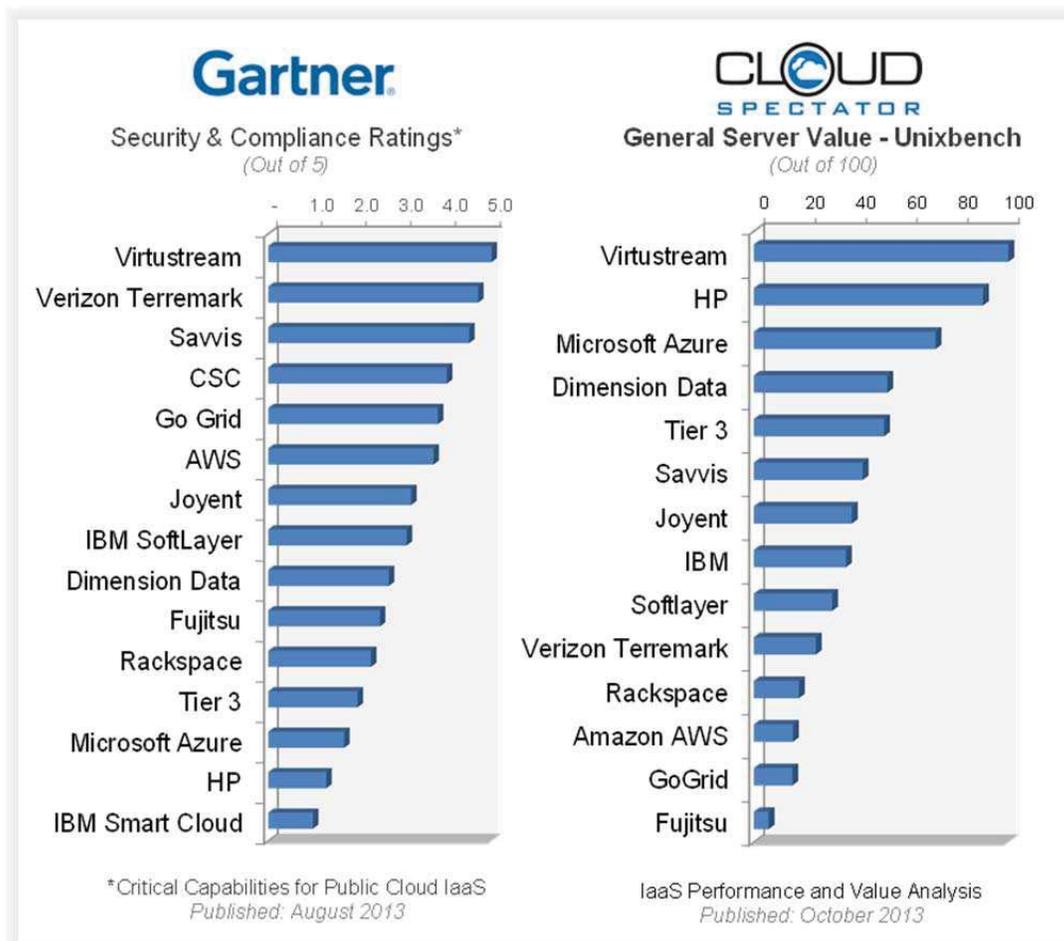
Virtustream's infrastructure is built to the most stringent requirements for compliance and security in order to support mission critical applications. Virtustream certification and processes meet or exceed NASPO's requirements, ensuring alignment with industry leading practices and ITIL type standards.

While Virtustream is able to provide best in breed services, the pricing model will present NASPO and subsequent Participating Entities with solutions at a cost effective rate. Since billing is based on a fractional unit of a traditional VM, Participating Entities will benefit from a truly elastic, consumption based model. This model aggregates utilization across all applications thereby delivering additional cost benefits and efficiencies for Participating Entities as the number of applications running on our IaaS platform increase.

Virtustream's focus on the enterprise is a key assets that will benefit the NASPO Cloud contract and Participating Entities that adopt the vehicle. The application service capabilities ensure that customers receive the maximum value of the cloud infrastructure. From onboarding, testing, managing and monitoring of your application environment, we can best enable Participating Entities to take advantage of the full potential of the enterprise cloud.

Backed by industry leading SLAs, and 7 x 24 Support, this proposal includes a replication solution across 2 data centers (both within the US) that provide Participating Entities with a very comprehensive and cost effective Disaster Recovery solution.

Key Benefits of the xStream Cloud Platform

1. **Guaranteed Resources** – Businesses require adequate computing capabilities that meet operational demand 24x7 without incurring the cost and maintenance burden associated with idle assets. Participating Entities will be provided with resources sold as infrastructure units with a guarantee that the required resources will always be available. Our Cloud solutions guarantee CPU, memory, network and storage I/O resources as defined by the number of µVMs a client commits to. We help our clients optimize the use of their virtual resources, with near real time usage statistics and trending analysis. The xStream platform goes a step further by also building in various levels of business continuity depending on the type of Infrastructure Units purchased.

2. **On Demand Resources** – Participating Entities will benefit from on demand resources which facilitate the ability to burst into additional short term compute resource capacity if required.

3. **Easy to Manage** – The xStream Portal provides role based access for clients to administer, monitor, control and report on their environment. The portal is an intuitive environment in which all client operations can be performed, securely, reliably and intelligently.

4. **Industry leading SLA's** – The xStream™ platform benefits from enterprise SLA's of 99.99% availability. The proposed SLA's for the xStream™ platform can cover the following elements of the service: Network Performance, Data Backup, Support response time, Physical security and 24x365 Engineering support. This is backed up by our full managed service capabilities.

5. **True Consumption Based Billing** - Virtustream is the only IaaS provider capable of provisioning compute resources based on aggregate workloads, thus providing the only true consumption based offering on the market today. Clients can purchase the amount of infrastructure resources they need as multi-tiered workload infrastructure units with integrated High Availability and Disaster Recovery.

Figure 4.   Virtustream Platform Overview
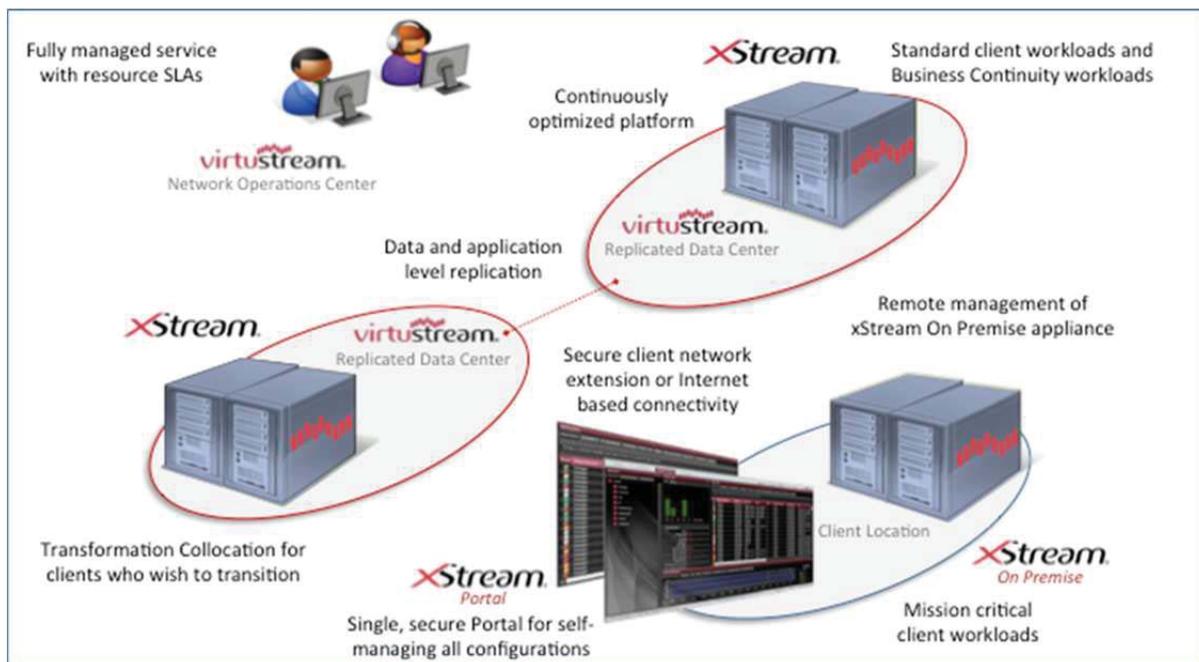
Backups will be taken to disk in primary data center and copied to the second data center for resilience. Full daily backups will be taken and kept for 30 days; one yearly full backup will be kept for seven years. All backups are synthetic full so only the changed data is copied to disk.

Virtustream Dual Data Center and Disaster Recovery Approach

Key Environment & Hosting components of the xStream® enterprise cloud:

- Fully virtualized solution including storage, servers and network I/O
- Guaranteed levels of performance for select tiers
- Consumption-based pricing
- Elastic and scalable
- Built in high availability and disaster recovery
- Proven on-boarding methodology
- Hosting with a SAP Certified cloud partner in a hardened US located data center with 24x7x365 monitoring and support staff and helpdesk
- Ability to tie charges back to departments or projects
- Service Level Agreement for all layers of solution

Consumption-Based Model

As opposed to the traditional billing by servers, where it is typical to see over provisioning of infrastructure resources, Virtustream pioneered the concept of a µVM with the intent to provide true consumption-based cloud provisioning. A µVM is logically defined as 200 megahertz (MHz) of CPU, 768 megabytes (MB) of memory, 40 IOPs of storage and 2Mbps of internal network bandwidth and eliminates the concern of virtual machine count and sprawl. This means that Participating Entities will only pay for the resources that they actually consume rather than allocated virtual machines.

Figure 5.   Consumption Based Pricing

IaaS Offerings

Virtustream offers 3 types of xStream® µVMs. They can be applied for different use cases as explained below.

- **Basic Plus µVM**: This µVM is for virtual machines where memory size is less than 64GB. For non-production workloads that do not require DR, use Basic Plus µVM, local storage, and replicated back-up. For production workloads that require DR, use Basic Plus µVM paired with Reserve (DR) µVM which reserves the same µVM capacity at the secondary data center so that in case of a DR event, the reserve µVM would be available for activation. Additionally, replicated storage and replicated back-up as well as provisioning the same network connectivity at the secondary site will enable a fully working system in case of a DR event.

- **High Memory Basic Plus µ**VM: This µVM is for virtual machines where memory size is greater than 64GB. Coupled with High Memory VM fee, High Memory Basic Plus µVM enables the customer less expensive rates for larger VMs. Currently the upper limit on the memory size is 1TB for High Memory VMs. The same approach applies for production and non-production workloads as explained above.

The proposed architecture is depicted in the following figure with two data centers.

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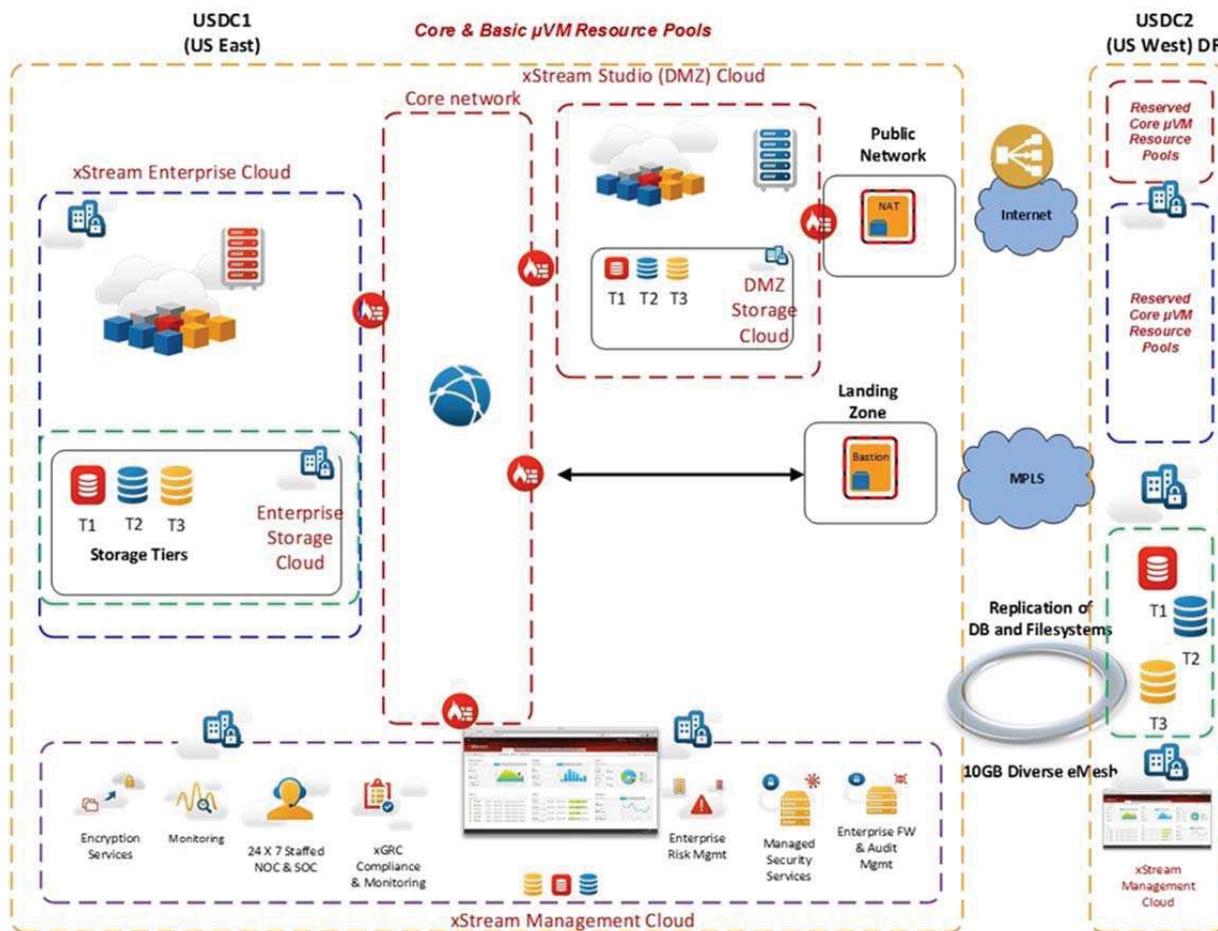
6.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

EMC Response: Virtustream's IaaS capabilities are fully audited at the data center level with SSAE 16 SOC 2/SOC3. The full report can be made available for the Participating Entities review.

Billing and Pricing Practices

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.

EMC Response: The description of billing and pricing practices is as follows:

Compute

Virtustream charges for compute consumption based on a unit of μVM. A μVM is a unit that is measured in 4 dimensions, CPU (200Mhz), Memory (.768GB), I/OPs (40), and Network (2 Mbps). These 4 are measured in 5 minute increments and the highest is picked. For example, a VM may consume 4 μVM's of CPU, 8 μVMs of Memory, 2 μVMs of I/OPs, and 1 μVM of Network. In this case, as 8 μVM's of memory consumption is the highest, this unit is selected. Then a five minute sampling is further averaged on hourly basis and further averaged so that monthly μVM consumption is determined.

Another distinction for our IaaS offer is that rather than measuring compute consumption on a per VM basis, we measure on a resource pool basis. The distinction is important because on a per VM basis, memory consumption may be at 60% utilization but in a resource pool basis, which takes into account memory share (which can be as high as 35%); the μVM consumption at a resource pool is about 30% less than the aggregate of the VM level consumption data. All of this means that the customer is charged on what is actually consumed and not an allocated basis. This approach to billing enables customers to enjoy savings unavailable to VM based billing methods.

Our IaaS offers 2 different types of μVMs which has different configuration characteristics and rates and we provide consumption data at VM and resource pool levels through its xStream portal.

Storage

Our IaaS offer has 4 Tiers of Block storage. The storage can be configured to be local only or local and replicated. Virtustream charges based not on allocated storage but on consumed storage as measured at the hypervisor. For example, a customer may create a VM with 30GB of storage. As seen from the VM, only 5GB is consumed of the 30GB. Then we will bill for the 5GB as do not charge extra for upload or download of data.

Back-up

Our offer provides two types of back-up: local only or local and replicated back-up with charges are based on protected data on a per VM basis. The size of the protected data varies based on the retention period of the back-up, generally 30 days for production workloads and 15 days for non-production and the change rate of the data.

Front End: Data that needs to be backed up — 100 GB

Protected: Amount nominally saved and restorable

5 Day retention, daily change rate of 5%

| 100 GB | 5GB | 5GB | 5GB | 5GB | **120 GB** |
| Day 1 | Day 2 | Day 3 | Day 4 | Day 5 | |
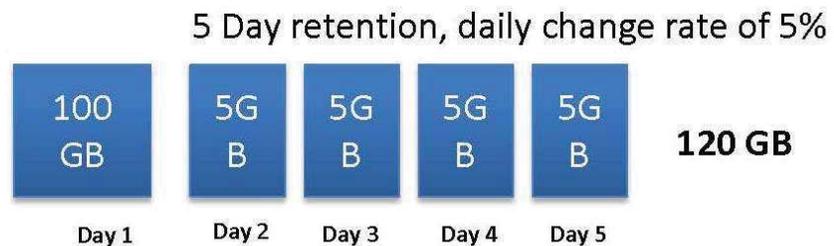
For network costs, our offer will only charge based on allocated and non-consumed network resources. For example, if a customer requested 10 Mbps network connectivity, then regardless of actual consumed network BW, customer is charged for the allocated BW.

All other services are charged based on discrete units either based on VMs or vCPU. For example, anti-virus service is charged on a per VM basis. Encryption is charged on a per vCPU basis.

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

EMC Response: Due to the unique basis of charge for compute, the customer should focus on actual utilization of the compute resources in terms of CPU and memory utilization. Having correct data will enable the customer to right-size the µVM consumption during pricing. We found that customers frequently overestimate the µVM consumption by not using empirical measurements resulting higher price estimate than actual. Additionally, customers can further reduce the consumption by turning off non-production workloads over weekends or evenings. This policy decision can also have a big impact on costs over time.

As Virtustream offers 4 tiers of storage, selecting the right tier can also create significant savings for the customer. Customers frequently overlook the cost of on-boarding and migration to a cloud. Depending on the complexity of the migration, this work may require a project based approach which we can support offer via our value-added services offer.

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.

EMC Response: Virtustream's IaaS solution is fully NIST compliant for *Essential Characteristics*, as the Infrastructure as a Service (IaaS) *Service Model*, with all deployment options – Private Cloud, Community Cloud, Public and Hybrid Cloud. To that extent:

- **On-Demand Self Service** - Our IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP.

- **Broad Network Access** - Our IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, etc.) which is growing rapidly as option for connecting cloud resources.

- **Resource Pooling** - Key to our solution is its proprietary and patented solution of µVM technology, which is effectively a granular solution for resource pooling, providing application performance, pay for consumption only and segregate resources for security and compliance, but aggregate for cost efficiency. In addition, Virtustream's IaaS is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and as we are able to configure and manage at the cluster and host machine level.

- **Rapid Elasticity** - Our IaaS is highly elastic through maintenance of buffers and users can use our self-service portal to self-provision, or via our web-based ticketing system to generate a service ticket, or the Technical Account Manager who is a customer's direct point of contact, to provision and de-provision resources and services. In addition, our solution also provides application level provisioning as part of its standard automation and orchestration tool.

- **Measured Service** - A significant advantage our IaaS solution is related to how we bill. Our solution takes average consumption of compute resources, thus Participating Entities would only pay for actual resources based on a monthly average. This is in comparison with a traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, the consumer of the cloud pays, but when it is down, they don't. In the case of our solution, a customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs. Our value-added services can also provide consultative and project support based on both a time and material or pre-negotiated statement of work.

- **Flexibility** - The deployment of our IaaS cloud solution can be on-premise or private based on a purchase of its Cloud Management Platform, Community Cloud based on its IaaS, Public Cloud based on its IaaS and Hybrid cloud based on its ability to provide software and IaaS combined.

Scope and Variety of Cloud Solutions

6.6 (E) SCOPE AND VARIETY OF CLOUD SOLUTIONS

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

EMC Response: The below information briefly describes our Virtustream Cloud Platform Services (CPS) offerings. These services are hosted in secure data centers in the United States and Europe, and comprise a range of Infrastructure as a Service (IaaS) platform capabilities, from compute, to storage, security, disaster recovery, and colocation.

IaaS Services

- IaaS Onboarding and Migration
- IaaS Compute (Virtual Machine)
- IaaS HANA Physical Appliances
- IaaS Storage / Backup
- IaaS Network
- IaaS Load Balancer
- IaaS Cloud & Storage Connect
- IaaS Ad Hoc Services

Security Services: Network Based (Perimeter Defense)

- Firewall
- IPSec VPN
- Intrusion Detection Service (IDS) - Network-level

Security Services: VM Based

- Anti-Virus / Anti-Malware (AV/AM) - VM-level
- Intrusion Detection Service (IDS) - VM-level
- File Integrity Monitoring (FIM)
- VM-Level Security Bundle (VLSB) - Includes AV/VM, IDS, and FIM
- Encryption
- Vulnerability Scanning
- Vulnerability Scanning
- Log Management
- Security Policy Auditing
- Two-Factor Authentication (2FA)

Best Practices

6.7 (E) BEST PRACTICES

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

EMC Response: Our IaaS core principle provides the highest level of security and offers customers choice related to the risk models. Currently, it is rated 5 out of 5 in the Gartner's Critical Infrastructure report compared to other IaaS providers identified in the Gartner Magic Quadrant. Due to the lowered risk of our security posture and our list of certifications customers have embraced our offerings and capabilities. For example, we work with departments within the US Federal Government (Department of Interior, Department of Transportation and others) as well as major Enterprises like Coca Cola. In addition, our solution provides complete visibility through its portal for all IaaS components; related to provisioning, pricing, monitoring and ticketing enabling Participating Entities to gain immediate status of their environment(s). Security, with compliance, data security and threat protection services are delivered as a service and per VM basis with a monthly recurring charge. Access to the environment is controlled using two factor authentication. Access can also be configured based on named users and security controls for our IaaS platform. This is described in the following section.

Cloud Platform Security

Our Cloud Platform Security (for the Infrastructure-as-a-Service environment) is designed, built, and operated to provide high levels of infrastructure security. Standard Services are used in our management environment and in all client environments including the following:

- All relevant employees use Mandatory Strong 2 factor authentication (2FA OTP) Administrative Access to all systems.

- Dedicated VLAN network segmentation and dedicated Virtual Route Forwarding (VRF) are used extensively to segregate environments and zones.

- Perimeter Firewalls are used to segment internal and external environments as well as segregate security zones. Configuration, monitoring, auditing and logging are included.

- Virtual Machine-based Firewall and Intrusion Prevention System (IDS) is installed on every virtual machine in the environment and is protected with Juniper's Security Gateway virtual firewall application and monitored service.

Security Services that are standard components for our IaaS management environment and are Optional Services for client environments including the following:

- Managed Two-Factor Authentication ("2FA") is in use for all application systems.

- Intel TxT Enabled Servers and Trusted Boot/Bios monitoring with Attestation Server and OS and VM support, including Geolocation and Geofencing according to NIST 7904 guidelines.

- Secure operating system (OS) builds based on DoD Secure Technology Implementation Guide (STIG) guidelines are used to build Virtustream's Management and Administration Servers.

- Server/File Integrity Monitoring (FIM) is installed in the PCI and IAAS clouds.

- Patching Regimen: Our offer includes patched host servers, network devices, security devices, servers and related services in the Management Network on a specified routine (monthly or quarterly, depending on release schedules), or when there is a CERT or other authorized source of patch that requires immediate attention. Based on urgency and risk of the issue we will schedule the patch as appropriate and use change control.

- Scanning regimen: vulnerability scanning is done on a monthly basis with additional 3rd party vulnerability scans done monthly. Additional scans are done when made aware of new vulnerabilities. Issues are classified and addressed according to Risk Classifications and are addressed with ITIL v3 change control processes.

- Managed IDS signatures are routinely updated and the logs are monitored.

- Anti-Virus is managed on all Management servers in Enterprise, PCI and, IAAS clouds.

- Logging Service of all servers, network devices, and security devices to a centralized log server system.

- Governance Risk Compliance: We use a complete Enterprise Risk Management toolset to manage compliance reporting and continuous monitoring to all of our supported compliance frameworks.

Cloud Platform Monitoring

Our offer monitors the cloud hosting platform for capacity, availability, response time, memory, storage capacity and IOPS, CPU utilization, networks and connectivity, and more. All of our tools, processes, and personnel are designed to support the new FedRAMP-required Continuous Monitoring Requirements, are SCAP certified, and will support FISMA Low, Moderate, and High (Future) impact environment requirements:

- Logging: All VPN access, Server syslog's, and all security tools logs are all aggregated, correlated, and exceptions analyzed.
- Log aggregation servers aggregate log data for analysis by our GRC, SEIM and Enterprise Risk Management Systems, and continuous monitoring tools.
- Our xStream software monitors CPU, Memory, IOPS, and network traffic statistics on per virtual machine, per host, per landscape, per customer, and per site levels.

Many other monitoring services are available as Optional Services for customer environments.

Security Awareness and Training Programs

We require mandatory security training for ALL IaaS relevant employees. The training will include modules on: Social Engineering, Email and IM, Social Networking, Browser security, Passwords, Encryption, Smartphones / Mobile Device, Monitoring / AUP, Data Privacy, and several dozen more topics.

We use the following training resources for our employees supporting IaaS:

- SANS Securing the Human - All Virtustream employees are required to complete this training which covers the following subjects: Social Engineering, Email and IM safe uses and practices, Incident Handling, HIPAA and PII, PCI-DSS, Privacy, EU Data Protection, and Computer Security Ethics.
- Due to our involvement with Federal Government customers, many of our US-based technical workforce has completed the following training requirements.
  - Federal Workforce Cyber Awareness
  - Department of Defense Privileged User Information Assurance Responsibilities

Privacy Policy

Our Privacy Policy is maintained online and has been vetted and approved by the US State Department "Safe Harbor" program.

Personally Identifiable Information ("PII") data management and provisions are included in an individual customer's managed services agreements to address federal and local laws and regulations, as well as the customer's information processing requirements.

Encryption Key Management

Our IaaS offer uses a strictly role based/accessed key management system for our management environments and offers this as an optional service for client environments.

- Encryption keys are maintained in a hardware security module (HSM) (both hardware based HSM and Virtual based HSMs). Access to the HSM requires multiple employees to eliminate single administration risk issues.
- Encryption keys can be provided to clients using an encryption key wrapper and using a hand-delivered physical security protocol.
- Our IaaS offer supports a very wide variety of key management processes: from our team managing the entire process to clients managing the entire process, as well as co-management of the key management process as per client specifications.

Customer and Zone Segregation

Our Enterprise Zone is the standard cloud service for most customer applications, security tools, and other supporting applications. The PCI Cloud and the Federal Cloud (IAAS) are physically and logically separated Zones for specific customer workloads and use cases.

Our Management zone is used exclusively by our staff to manage the health, backups, security tools capacity planning, and SLA monitoring tools. It is operated and maintained to the requirements of FISMA moderate and FedRAMP requirements.

Documentation

We maintain all documentation for security and compliance requirements within its Management systems and for the data center facilities.

We can provide documentation for specific security and compliance requirements for customers, generally as an optional service, defined in an individual customer's managed services agreement.

Data Encryption

Our offer uses encryption at critical points within our cloud platform infrastructure, all of which are offered as an optional service for customer environments:

- **FIPS**: All encryption technologies are FIPS 140-2 certified.
- **In Transit**: IPSEC VPN's using AES256 bit encryption.
- **At Rest**: Managed Encryption using AES256 bit encryption, or a customer-specified tool as agreed upon in the customer's managed services agreement.
- **In Archive**: Backup systems use AES256 bit encryption.
- **Before Move**: Agents can be installed on servers located at client locations to manage and encrypt data before movement to our IaaS cloud.

Authentication

Our IaaS offer supports identity federation standards (SAML, SPML, and WS-Federation) as a means of authenticating/authorizing users and the xStream portal implements the SAML v2 standard, all as an optional service for client environments.

- All IaaS relevant employees are required to use our SafeNET MobilePASS OTP strong two-factor authentication ("2FA") systems. This is an optional service for client environments.
- Role-based security and access is maintained in xStream Identity Management Modules and Subsystems.
- Identity management systems included in the xStream portal enable role-based and context-based entitlement to data (enables classification of data for a tenant).
- Our offer can support either customer-preferred multi-factor authentication tools for user access (digital certs, tokens, biometric, PKI, etc.) or customers can leverage our tools.
- PIV card support is typically managed by the Federal Agency using the system.

EMC²

SECTION 5 – ORGANIZATION PROFILE

Contract Manager

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.

EMC Response: The table below identifies the Contract Manager that will serve as the single point of contact for management of the NASPO ValuePoint Master Agreement:

Table 7.   Primary Contact Information for Contract Manager

Name:	Kristine French
Telephone #	(916) 797-7044
Email Address	kristine.french@emc.com
Work Hours:	8:00 am – 5:00 pm Pacific

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.

EMC Response: Kristine French, EMC NASPO ValuePoint Contract Manager, will be dedicated to managing the EMC NASPO ValuePoint Cloud contract. Ms. French has 19 years' experience managing and administering Public Sector Contracts. Ms. French will have the authority to enforce the scope of work, restrictions, and terms and conditions of the resulting contract. She thoroughly understands the Participating Addendum process as she managed the successful implementation of EMC's NASPO ValuePoint Data Communication Contract AR620 and NASPO ValuePoint Computer Storage Contracts MNWNC-109, resulting in 49 Participating Addendums nationwide.

EMC has provided the resume for Kristine French as an attachment to the technical proposal titled "Kristine French Resume 2016.pdf".

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.

EMC Response: Kristine French, EMC NASPO ValuePoint Contract Manager, will be dedicated to administering the NASPO ValuePoint Cloud contract. Ms. French will have the authority to enforce the scope of work, restrictions, and terms and conditions of the resulting contract. This role includes implementing the rollout plan for the contract nationally. Ms. French will develop and manage the communication, implementation and administration plans to successfully coordinate pre negotiations and post negotiation activities with Participating Entities. Ms. French will manage the oversight of compliance, order tracking, ad hoc report requests, and filing all reports. Additionally she will oversee the VAR Approval process and the development and delivery of training and marketing materials. Ms. French is the contract liaison for the EMC Public Sector legal team, pricing and service schedule updates, product categorization, pricing verification, and back-office support.

SECTION 6 – TECHNICAL RESPONSE

This section should constitute the Technical response of the proposal and must contain at least the following information:

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

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

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

Technical Requirements

If applicable to an Offeror's Solution, an Offeror must provide a point by point responses 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 Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.

EMC Response: The IaaS offer to the State and Participating Entities is based on Attachment D; Our IaaS solution can provide differentiated security solutions for "Low", "Moderate" and "High" risk resources. Customers will be able to select security postures based on their own risk assessment. Related to this is that our IaaS offering is NIST compliant for *Essential Characteristics*, as the Infrastructure as a Service (IaaS) *Service Model*, with all deployment models – Private Cloud, Community Cloud, Public and Hybrid Cloud. Features include:

- **On-Demand Self Service** - Our IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP.

- **Broad Network Access** - Our IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, etc.) which is growing rapidly as an option for connecting cloud resources.

- **Resource Pooling** - Key to our solution is its proprietary and patented solution of µVM technology, which is effectively a granular solution for resource pooling, providing application performance, pay for consumption only and segregate resources for security and compliance, but aggregate for cost efficiency. In addition, Virtustream's IaaS is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and as we are able to configure and manage at the cluster and host machine level.

- **Rapid Elasticity** - Our IaaS is highly elastic through maintenance of buffers and users can use our self-service portal to self-provision, or via our web-based ticketing system to generate a service ticket, or the Technical Account Manager who is a customer's direct point of contact, to provision and de-provision resources and services. In addition, our solution provides application level provisioning as part of its standard automation and orchestration tool.

- **Measured Service** - A significant advantage our IaaS solution offers related to how we bill. Our solution takes average consumption of compute resources, thus Participating Entities would only pay for actual resources based on a monthly average. This is in comparison with traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, consumer of the cloud pays, but when it is down, they don't. In case of our solution, a customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs. Our value-added services can also provide consultative and project support based on both a time and material or pre-negotiated statement of work.

- **Flexibility** - The deployment of our IaaS cloud solution can be on-premise or private based on a purchase of its Cloud Management Platform, Community Cloud based on its IaaS, Public Cloud based on its IaaS and Hybrid cloud based on its ability to provide software and IaaS combined.

Based on customer risks, our IaaS Cloud delivery model will be able to offer security capabilities that address low, moderate and high data risk levels.

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

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

EMC Response: Our IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP. Virtustream portal that enables the user to provision VMs, order services through a catalog, add storage, upload service templates, and run various reports all through the same portal.

The xStream Portal is our cloud management interface that allows users to monitor and manage their virtual datacenters through a single pane of glass:

- Two-factor authentication (username, PIN and one-time-passcode)
- Centralized portal views are determined by the roles assigned to the user
- Capabilities available via the portal:
  - Environment Summary
  - Consumption view/reports (billing)
  - Catalog of Services-Products / Catalog Orders
  - Workflow approval process
  - Service Level Availability adherence and reporting
  - Events (user/system initiated activity) / Log
  - Profile driven deployments
  - Offering driven deployments (managed by profile)
  - Manage/Assign templates
  - Application Automation and Orchestration
  - Supply Chain Management for Cloud Resources
  - Compute/Network views/reports

Figure 7.   xStream Portal Sample View

- xStream Optimization Tool
  - Capacity planning service that provides resource pool consumption forecasts for resource pools managed by xStream
  - Probabilistic view of future consumption in each resource pool
  - Strategic over/under provisioning engine
    - Allows forecasting for over or under provisioning a resource pool

Figure 8.   xStream Optimization Tool Sample View

EMC Response: Our IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, etc.) which is growing rapidly as option for connecting cloud resources.

EMC Response: Key to our solution is its proprietary and patented solution of µVM technology, which is our granular solution for resource pooling. This technology provides high quality application performance and saves customers costs since Participating Entities would only pay for consumption. In addition our resource pooling technology segregates resources allowing compartmentalized security and compliance based on the Participating Entities chosen environment. In addition, our IaaS offer is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and getting down to cluster and host machine level. The resources are pooled based on the following specific criteria:

- **ONLY Accessible Using Private Network** – We call this pool "Enterprise" which most of our IaaS workload is residing. There is no direct access from Internet into this pool. This is protected via a pair of routing and firewall from any other zones.

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

EMC Response: Virtustream provides Rapid Elasticity based on Compute, Storage, Network and Security as the customer needs, mostly on demand basis. It allows for growth of existing resources as well as provisioning of new resources. Virtustream's self-service portal, ticketing system and also the Technical Account Manager, who is the single point of contact for Participating Entities allows for provisioning and deprovisioning of resources and services. In addition, Virtustream is uniquely positioned to provide application level provisioning as part of its standard automation and orchestration tool. Resources can be scaled based on application size, memory, storage, network requirements. xStream utilizes a supply chain to define resource profiles, attributes and offerings than can be provisioned.

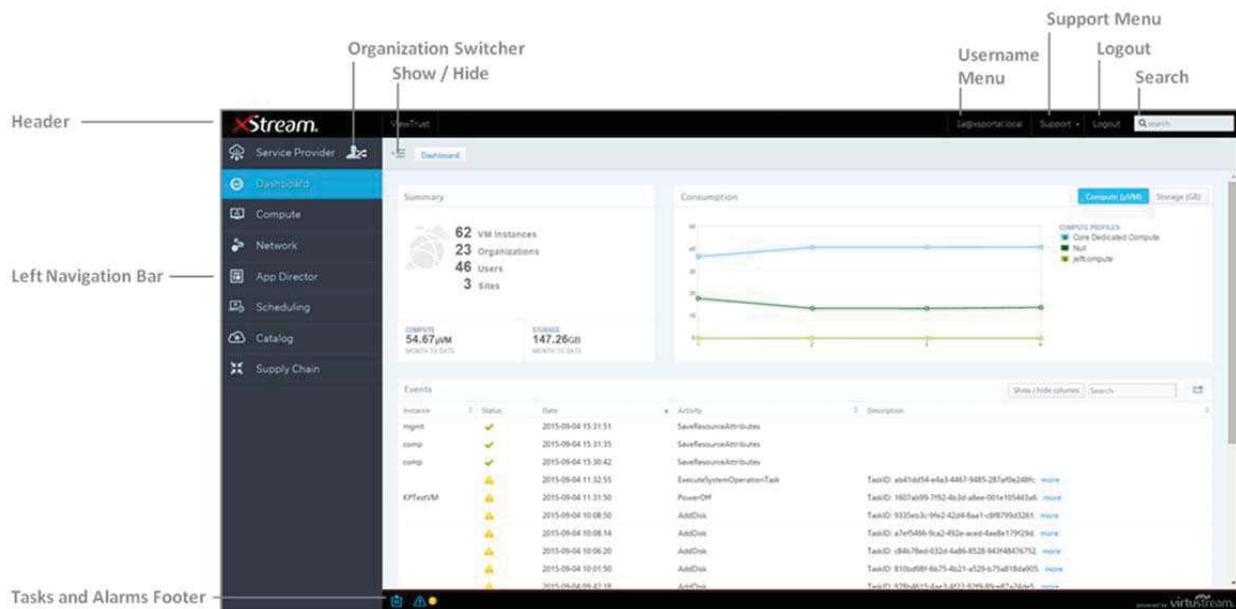> *8.1.2.5 NIST Characteristic - <u>Measured Service</u>: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.*

EMC Response: Our solution is based on µVM Technology, which allows for measured services to be accurately captured so only consumed resources are billable. The Virtustream solution takes average consumption of compute resources, and Participating Entities would only pay for actual resources based on a monthly average. This is in comparison with traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, consumer of the cloud pays, but when it is down, they don't. In case of the our offer solution, customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs; also, we can provide consultative and project support based on time and materials.

The µVM brings significant benefits: enabling application level performance SLAs – which an average VM cannot. µVMs eliminate wasted headroom in fixed size VMs, generating significant efficiency improvements (up to 40% beyond traditional virtualization) and our IaaS offer would only charge by the µVM so you only pay for the resources you actually consume not what you might need. Using µVMs also enables applications to be used across multiple hypervisors, across multiple clouds and between different locations – enabling true hybrid clouds. µVM technology allows us to offer enterprise class clouds capable of running both mission-critical enterprise applications and web-scale applications, delivering the full benefits of cloud to the enterprise.

Figure 9. The µVM Model Enables Cloud Efficiencies

µVMs optimize utilization of data center assets within and across physical locations. It is proven to be extremely efficient with large, complex workloads, reducing total cost of ownership (TCO).
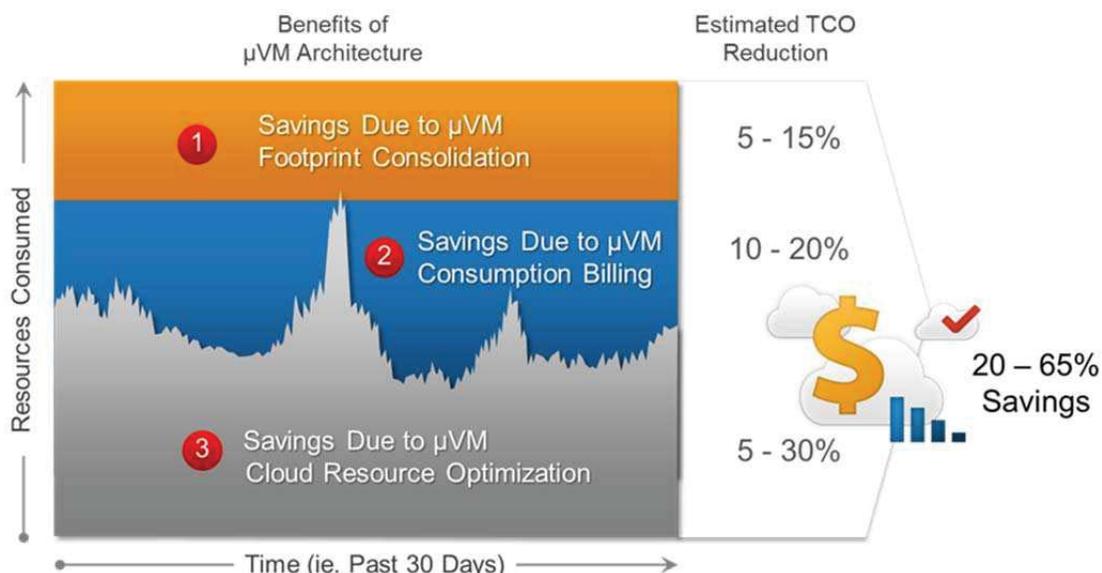
A µVM manages and measures the consumption of compute resources based on actual usage rather than allocated basis. The traditional method measuring of compute resource consumption is by allocation (e.g. 4GB RAM VM). With µVM, we measure the actual consumption of compute resources within the 4GB RAM VM. A µVM is measured at 768MB of RAM or 200MHz of CPU, whichever is higher. We have found empirically that a 4GB VM typically consumes 2.2 µVM, which translates to 1.7GB of RAM usage. Therefore, instead of paying for the entire 4GB of RAM, you only pay the consumed amount of 1.7GB.

True Consumption

EMC's Virtustream IaaS offer has pioneered a true consumption-based Cloud platform based on our patented µVM technology. This technology allows Virtustream to optimally place the workloads and manage the xStream Enterprise Cloud infrastructure, and measure our customers' actual consumption of resources within the cloud. Unlike other cloud providers that will require Participating Entities to pay for the "T-Shirt" size VM or the allocated resource pool, Virtustream's µVM model allows customers to allocate the resource pool for the peak consumption over a monthly period, however, the bill is based on a 5-minute average consumption over the course of the month. The solution we have proposed leverages this unique technology we have developed.

Figure 10. Our Unique Approach: The µVM

Our patented µVM ("Micro virtual machine") technology changes the way infrastructure resources are provisioned, managed and metered. The impact on efficiency can be compared to that of electricity.

How do you want to pay for your Cloud?

Appliance Power Ratings?   Individual Circuits?   Actual Kilowatts Consumed?

LEAST COST EFFECTIVE   MOST COST EFFECTIVE

Physical Servers:
Pay When in Use or Not

Applications are dedicated to physical hardware. Typical of traditional enterprise IT.

Virtual Machines:
Pay in Full When Powered On

Virtualized applications share hardware. Typical Model for Public Cloud IaaS Providers.

µVM Consumption:
Pay Only For Actual Total

Virtualized applications optimized to the smallest footprint possible. Pay only for total µVMs used.

Guaranteed Performance & Elasticity

EMC's Virtustream IaaS Cloud offer is designed to deliver performance at every layer of the infrastructure. The commitment performance is backed up by performance SLA's cover compute, storage and networking for all workloads. In the event customers request our Cloud Cover Services (Managed Services) for Application, we include an SLA for application availability. Our IaaS will provide Participating Entities with a robust storage solution with latency-based storage SLA's, allowing customer workloads to burst to high I/O demands without experiencing performance degradation. These features and capabilities provided to Participating Entities will allow the IT and Business organization to receive better performance in the Virtustream xStream Enterprise Cloud and without the expensive cost of a dedicated storage solution. This is illustrated in the following figure.

Figure 11.   Storage Tiers Align Cost with Performance
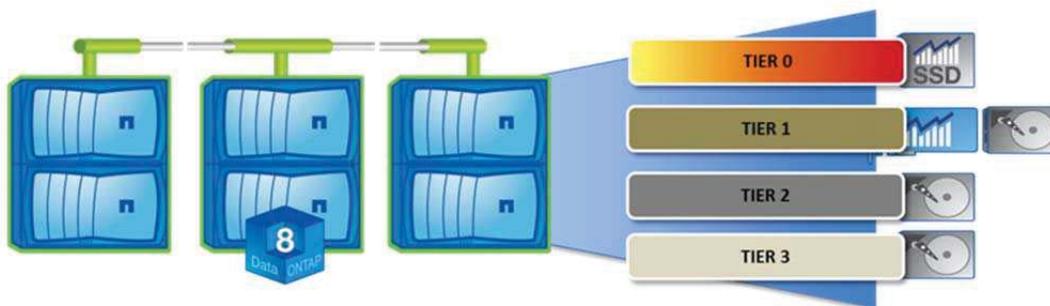
STORAGE TIER	RESPONSE TIME SLA	AVAILABILITY SLA	STORAGE MEDIA	ADD-ON FEATURES	APPLICATION USAGE
Tier 1	<10 ms LATENCY	99.999%	15K SAS DRIVE 200GB SSD	QoS PRIORITY FLASHCACHE	HIGH TRANSACTION DATABASE
Tier 2	<20 ms LATENCY	99.999%	15K SAS DRIVE	FLASHCACHE	STANDARD DATABASE & APP
Tier 3	Best Effort	99.999%	10K SAS DRIVE		STANDARD APPLICATION

Virtustream's xStream cloud is agnostic to the workload and supports over 1,700 different x86 applications. In fact, blending workloads comprised of different compute characteristics such as CPU, memory, and IOPs are ideal for Virtustream's µVM technology. Blending these workloads yields the highest cost efficiency for our Customers. The following is an example of blending workloads, one that is IOPS dominant and a second that is RAM dominant. The end result is an initial savings of over 36% for normal workloads and almost doubles that for workloads that require Disaster Recovery.

Figure 12. Datawarehouse - µVM Profile

Combination of all Workload resources
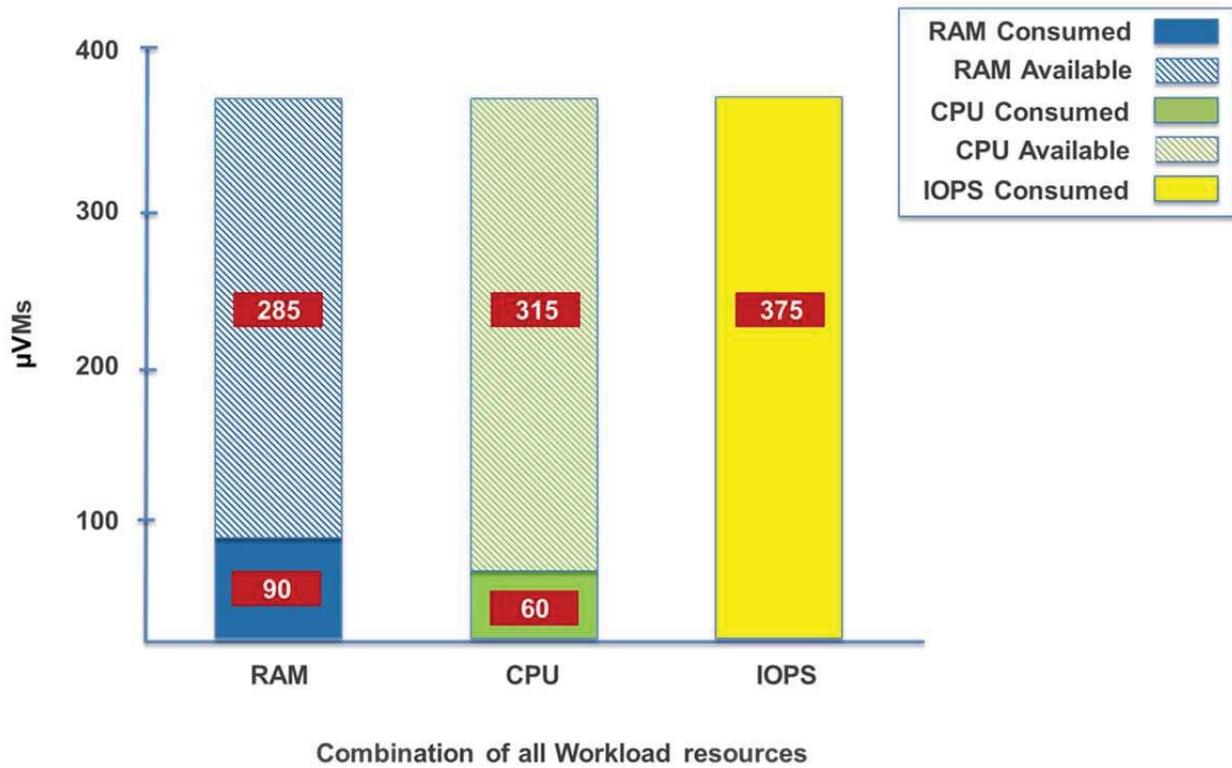
Datawarehouse Workload – IOPS Dominant

- **CPU**: 60 µVMs consumed
- **RAM**: 90 µVMs consumed
- **IOPS**: 375 µVMs consumed

Figure 13.   SAP Workload - µVM Profile

Combination of all Workload resources
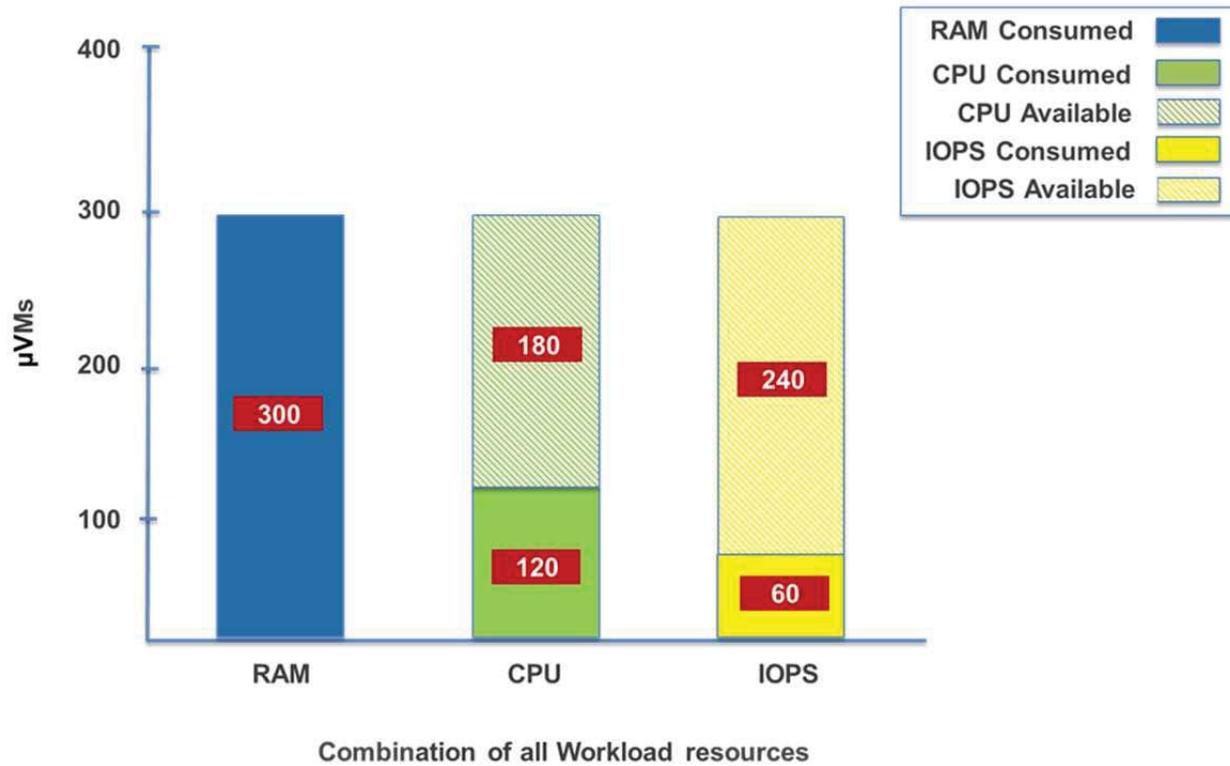
SAP Workload – RAM Dominant

- **CPU**: 120 µVMs consumed
- **RAM**: 300 µVMs consumed
- **IOPS**: 60 µVMs consumed

Figure 14.   Blended Workloads - µVM Profile

Combination of all Workload resources
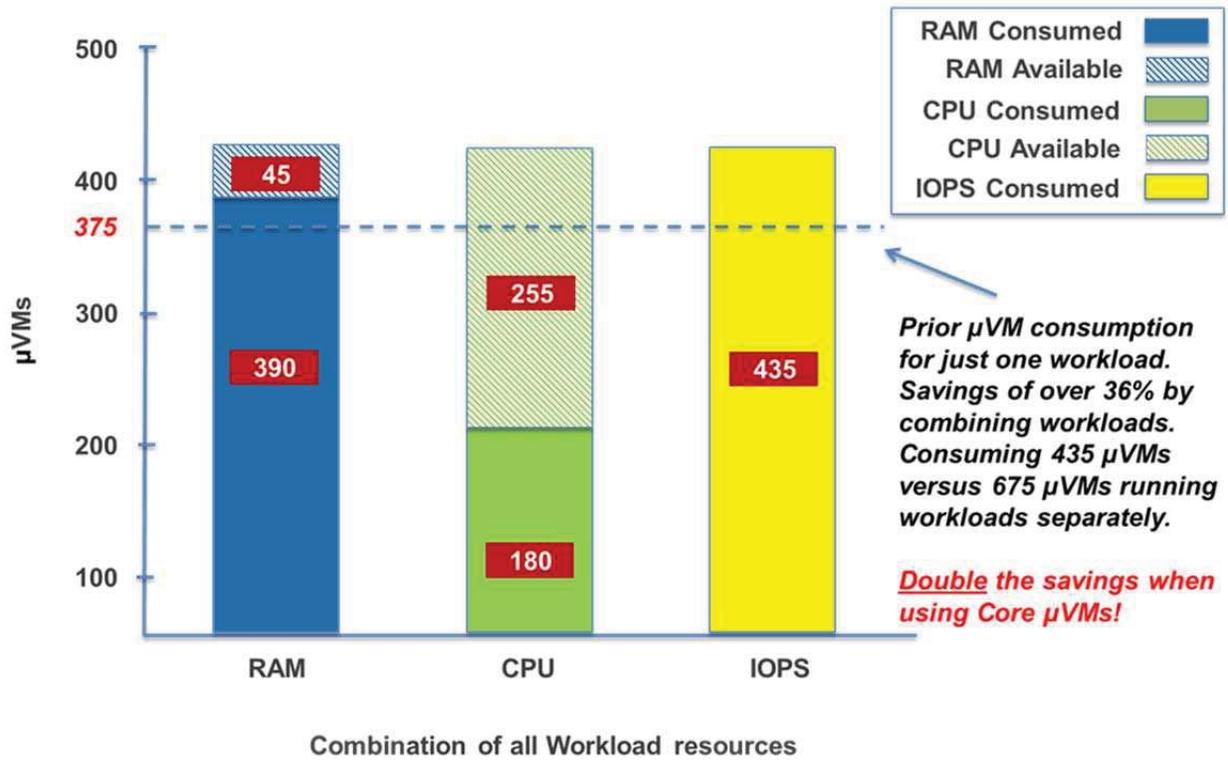
Blended Datawarehouse (IOPS dominant) and SAP (RAM dominant) Workloads

- **CPU**: 180 µVMs consumed

- **RAM**: 390 µVMs consumed

- **IOPS**: 435 µVMs consumed

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

EMC Response: Our Infrastructure as a Service (IaaS) offering is focused on mission critical workloads and applications.

The solution provided as part of this response is IaaS only. Our IaaS is targeted for all virtualized, x86 based cloud solution. While we have secured and segmented infrastructure for FedRAMP, FISMA, PCI and other regulated workload, it is best suited for any and all enterprise workload as long as the workload can be virtualized and run on x86 platform. For non x 86 environments, our offer provides Collocated areas, which is cross connected with the cloud.

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

EMC Response: As described above in 8.1.2.1 to 8.1.2.5, our Virtustream IaaS offer complies with Attachment C & D, where the NIST Service Model as well as the Scope of Services has been defined with its current offering.

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

EMC Response: In the first section of the Attachment D, where the categorization of the services are defined based on risks, we can provide controls to adhere to the policy of Participating Entities for governance, risk and compliance. The security controls can be provided per VM basis, as well as for the whole environment. In addition, in can also be provided for segregated workload, individually and for that specific workload.

In terms of the compliance with the NIST definition, the details are listed in 8.1.2.1 to 8.1.2.5.

Subcontractors

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.

EMC Response: EMC will be providing cloud solutions directly. EMC is a federation of companies that offer a variety of services. The IaaS services under this contract will be provided through our wholly-owned subsidiary, Virtustream, Inc. and from EMC-owned data centers.

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.

EMC Response: EMC will be providing the services directly and through its wholly-owned subsidiary, Virtustream, Inc.

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.

EMC Response: EMC does not intend to use subcontractors.

Working with Purchasing Entities

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;*

EMC Response: Virtustream Incident Response, Security Operations, and Operations personnel will be involved with data breach resolution. Examples of incident response personnel include Tier 1 and Tier 2 Service Desk Personnel, the Director of Security and Compliance, Data Center Manager(s), Security Architect, and Security Engineers/Analysts. The Purchasing Entity shall communicate all Data Breach points of contact with Virtustream before production workloads are in place. This ensures Virtustream's security teams are able to communicate with the

Participating Entities during and after the breach. All communications with the Participating Entities will be streamlined through a centralized person or focal group from Virtustream. As a member of the Virtustream Incident Response team, the Contract Manager will serve as the point of contact who will provide status updates to the purchasing entity.

- *Response times;*

EMC Response: Response times for data breach are negotiable and customer dependent.

- *Processes and timelines;*

EMC Response: Data breach processes and timelines are customer dependent and negotiated prior to production workloads onboarded to Virtustream's IaaS. Virtustream does not control access to a customer's network or environment. Participating Entities are responsible for communicating with Virtustream security personnel if they detect a breach within one hour.

- *Methods of communication and assistance; and*

EMC Response: Virtustream's primary mode of communication with a Participating Entity during a breach will be via telephone. The secondary mode of communication is via email. Participating Entities are required to provide primary, secondary, and tertiary points of contact prior to production workloads going live. The points of contact shall include primary phone number/email address and secondary phone number/email address. This information shall be included in the Participating Entity's data breach or incident response plan and provided to Virtustream.

- *Other information vital to understanding the service you provide.*

EMC Response: None.

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.

EMC Response: Virtustream does not release customer information or contact information as we do not have access to customer data.

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

EMC Response: Virtustream will provide a test/development environment that will be identical to the customer's production environment.

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

EMC Response: As provider of IaaS, Virtustream provides a customer portal (a.k.a. xStream Portal) which enables customers to access the performance and consumption data of its IaaS resources, provision and deprovision IaaS resources, and open and check the status of the service and trouble tickets. While this portal is accessible through a wide variety of browsers, this portal has not been enabled for Section 508 compliance.

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

EMC Response: As Virtustream is a provider of IaaS only, Virtustream is not responsible for how its customers choose to access their content. However, we do provide a customer portal (xStream Portal) which enables customers to access the performance and consumption data of its IaaS resources, provision and deprovision IaaS resources, and open and check the status of the service and trouble tickets. The xStream portal currently supports Internet Explorer v11, Chrome (latest released version), Firefox (latest released version) and Safari v8.

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.

EMC Response: During the solutioning phase which occurs prior to SLA execution, our cloud architects (CT6) will meet with NASPO customers to develop the optimal solution based on the customer requirements. As part of the overall design, Virtustream will provide compliance guidelines and solutions for security standards such as HIPAA, PCI, FedRAMP, and ITAR. Virtustream's security compliance expertise is limited to the security standards that Virtustream cloud currently meets.

To further ensure that Virtustream's compliance guideline is correct, Virtustream conducts an internal solution review process.

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.

EMC Response: Virtustream understands that Participating Entities are likely looking to transition their applications to cloud providers. The provisioned virtual systems will provide high availability of the production environment for all associated topology components. Included in the design will be disaster-recovery capability, planning, and management which will be driven by the agreed upon service level agreements (SLAs).

The Virtustream proposal will provide a portal for Participating Entities to monitor performance, assign capacity, billing and problem resolution of all provisioned systems. If desired and applicable, system performance, as experienced by Participating Entities' users, will be within a specified range also detailed as part of the SLAs and Statement of Work (SOW) / Order Form.

Virtustream will ensure compliance with all Participating Entities' security and other regulatory requirements that may exist and will provide the supporting documentation. All contracts executed between Participating Entities and Virtustream will be based on a consumption model. Virtustream will work with Participating Entities to integrate with Participating Entities' service desk.

Virtustream has optimized an implementation methodology we call the Cloud Transformation Program. In this program, we have project plan templates that complement the methodology and ensure all critical aspects of an implementation are fully planned, and that quality gates are in place for movement from phase to phase.

At project kick-off, Virtustream and a Participating Entity will develop a detailed Implementation Plan, on a system-by-system, week-by-week basis, to ensure that both sides of the relationship have clear expectations on what is to be accomplished, by whom, and in what timeframe. Upon completion of the Implementation Plan, Virtustream and the Participating Entity will establish a Project Governance Plan and the Project Governance Plan will manage

Implementation Plan and ensure alignment at all tiers of the organization, define expectations for status update frequency and formats, and establish an escalation path for issue identification and resolution.

Figure 15.   Sample Work Plan

Our team will participate in the Organization Change Management process that will be led by Participating Entities. Our team will participate in the design of the Change Management process, including providing Participating Entities with best practices and lessons learned based on previous experience, guidance to Participating Entities executive team on risks, support communications to the organization led by Participating Entities, and collaboration on the detailed Implementation Plan and project Governance Board to ensure the successful implementation of the initiative.

For the operational change, our team will lead Participating Entities through cloud onboarding process, train Participating Entities on the cloud management portal and administration tools, and provide service desk orientation to the Virtustream Enterprise-Class Cloud. During the onboarding process, we will work with Participating Entities to create service run-books, to customize the standard templates for Participating Entities cloud services and company culture.

Our migration practice principles are as follows:

- We follow application specific migration guidelines, best practices and procedures for the migration process and target environment configuration.

- We maintain best practices, configuration templates, STIGs, and lessons learned for its engineers and customers to leverage for optimal performance and security in a virtualized environment.

- Our procedures ensure that data is correctly converted and the systems maintain application support after go-live.

Relationship Management / Contract Governance

Our team will work collaboratively with Participating Entities to develop / maintain a relationship structure that leads to quick resolution, regularly scheduled status meetings, and quarterly business reviews.

Our IaaS team will assign multiple key personnel to Participating Entities including an Executive level sponsor. The primary point of contact will be Virtustream's Technical Account Manager (TAM). The TAM is responsible for daily activities/interaction and understanding/ensuring Participating Entities objectives are met at a minimum. Optimizations and other improvements to processes/standard operating procedures are delivered by the TAM in coordination with other Virtustream staff working behind the scenes. The TAM will coordinate day-to-day operation, service level management and SL reporting.

The following outlines our approach to service desk escalation and issue resolution:

Escalations within Virtustream

Our offer will provide Level 0 and Level I support and first call resolution where possible, as determined by Virtustream. Where first call resolution is not possible, the Virtustream Service Desk provides incident management for Incidents and Urgent Service Requests escalated to Level II and Level III resources as defined below.

In the event that Virtustream's Response to an Incident is not acceptable to the Customer, Customer can contact the Virtustream Service Desk and request escalation to the head of the Service Desk. We shall, upon receipt of any such request, immediately escalate the issue to the head of the Service Desk or technical team as appropriate.

Service Request Prioritization

Service Requests are assigned a priority of either 'Urgent' or 'Standard' and are queued for fulfillment with the corresponding priority. All Service Requests will be reviewed by the Virtustream Service Desk, who will determine the appropriate priority to assign with collaboration of Customer.

Incident Prioritization

All Incidents that are reported to the Virtustream Service Desk or that Virtustream otherwise becomes aware of, will be initially assigned a priority by the Virtustream Service Desk as set forth below. Internal escalation for Incidents to Level II and Level III resources are based on the priority level assigned to the Incident.

Table 8.   Incident Prioritization

INCIDENT PRIORITIZATION		
PRIORITY/ SEVERITY	**DEFINITION**	**RESPONSE TIME SERVICE LEVEL**	
1	Major part of the system is unavailable/not operating correctly, affecting multiple users. No workarounds in place and business operations are not possible. **Or** Incident has a critical impact on the business (e.g., loss of the Exchange Production server impacting all users).	**30 minutes**	Response time will be within indicated time beginning from when the customer creates a ticket or a monitoring event is validated. Additional resources are engaged via Virtustream's on Call Process.
2	Part of the system is unavailable/not operating correctly, affecting users in a single function. No workarounds in place and business operations in this function are not possible/severely impacted. **Or** Incident has a serious impact on part of the business (e.g., a configuration change is impacting a small subset of users).	**60 minutes**	
3	Part of the system is unavailable/not operating correctly, affecting users in a single function. Workarounds in place, but business operations are impacted, although not severely. **Or** Incident has a temporary impact on users and is non critical or is a development issue (e.g., email is slow to deliver)	**4 hours**	
4	Incident that is causing inconvenience to the business, but not impacting operations. **Or** Incident has a minor impact on users or business, or issue is a request for further information	**1 business day**	

We will assign a Technical Account Manager starting on day 1 of the contract. The Cloud Platform, Cloud Cover (managed services), and Cloud Security team's will also be assigned to a Participating Entity upon execution of the contract. All of the individuals assigned to the Participating Entity's account have significant years of experience in their fields.

The TAM assigned to a Participating Entity will provide reports ad hoc but also on a quarterly basis. The quarterly business reviews include but are not limited to performance measurements, service requests. On a monthly basis, the TAM will provide a consumption report detailing the items consumed by each virtual machine. This delivers a very granular cost breakdown to Participating Entities which will allow the data to be carved multiple ways. Also, information can be gathered by the Participating Entity's team any time they want from the xStream portal. A Participating Entity can also issue a ticket to Virtustream operations center to request information as well. The TAM will conduct scheduled meetings and be in constant contact with Participating Entities. The TAM is an extension of the Participating Entity's team.

Our team performs a Root Cause Analysis (RCA) and document in writing (with Virtustream and approved by Customer), to diagnose problems at the lowest reasonable level. This process includes a report of the corrective action to be taken and defined timelines for corrective actions, which shall eliminate, to the extent reasonably possible, repeat failures. The following details the Responsibility Assignment Matrix (RASCI) for RCAs:

Table 9.   RASCI for RCAs

ROLE/FUNCTION	CUSTOMER	VIRTUSTREAM
Request Root Cause Analysis tickets by contacting the Virtustream TAM (Customer requests Incident report/Problem record)	R/A	S
Document, track and manage all Problem tickets using ITSM system	S	R/A
Provide Problem management review and Root Cause Analysis (RCA) for all in-scope P 1 Incidents (preliminary report within 48 hours; final within 15 calendar days)	S	R/A
Provide Problem management and RCA of identified Problems (e.g., reoccurring events, alerts) - investigate and diagnose	S	R/A

RASCI Definition:

- **R:** Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
- **A:** Accountable is the authority that approves the work of "R" before it is effective.
- **S:** Support "R" as necessary to complete the task or deliverable.
- **C:** Consulted reviews output or progress necessary to complete the task or deliverable.
- **I:** Informed needs to be notified of results, completion, or deliverable but need not necessarily consulted.

Customer Service

8.4 (E) CUSTOMER SERVICE

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

- *Quality assurance measures;*

EMC Response: Virtustream provides 24/7/365 Support Center (xOC) via Phone or email to escalate issues or questions into for support. The xOC provides ongoing customer support and metrics on a per customer basis to support trending and proactive analysis of customer issues. Additionally Virtustream supplies Technical Account Managers (TAMs) as an option to support a dedicated account representative who can provide ongoing analysis and suggestions back into the business for recommendations and providing a single point of contact to engage with planning and issue support.

- *Escalation plan for addressing problems and/or complaints; and*

EMC Response: Virtustream provides 24/7/365 Support Center (xOC) via Phone or email to escalate issues or questions into for support. Any operational issues that are immediate in nature should follow this route for incident management procedures to open and log the request for prompt attention. The processes of addressing any issues or complaints of a non-production and or non-technical (People Process) issues should be directed to the account TAM or into the xOC management staff to support being able to facilitate direct dialogue with the requesting group or individual. Virtustream takes overall customer satisfaction of paramount importance and will setup discussions with the leads and managers within the xOC operations staff to support any customer problem or issue.

- *Service Level Agreement (SLA).*

EMC Response: Service Level Agreements are as follows:

Table 10. Enterprise Level Agreements

TICKET PRIORITY	VIRTUSTREAM SLA TIME TO ASSIGN (TICKET ACKNOWLEDGEMENT)	VIRTUSTREAM SLO TARGET RESPONSE TIME (TECHNICAL RESPONSE)	VIRTUSTREAM SLO TARGET RESOLUTION (ISSUE RESOLUTION)
Priority 1	5 minutes	1 hour	8 hours
Priority 2	5 minutes	8 hours	1 day
Priority 3	5 minutes	24 hours	5 days
Priority 4	5 minutes	48 hours	7 days

Table 11. Self-Service/Standard Level Agreements

TICKET PRIORITY	VIRTUSTREAM SLA TIME TO ASSIGN (TICKET ACKNOWLEDGEMENT)	VIRTUSTREAM SLO TARGET RESPONSE TIME (TECHNICAL RESPONSE)	VIRTUSTREAM SLO TARGET RESOLUTION (ISSUE RESOLUTION)
Priority 1	30 minutes	2 business hours	8 business hours
Priority 2	30 minutes	8 business hours	48 business hours
Priority 3	30 minutes	3 business days	5 business days
Priority 4	30 minutes	5 business days	7 business days

Table 12.   Service Level Definitions

	DEFINITIONS
1	SLO is a Service level objective, which is a target timeframe.
2	SLA is a Service level agreement, which is a contractual, agreed-upon timeframe.
3	Time to assign indicates the timeframe to send automated system acknowledgement that the ticket has been logged and assigned.
4	Target response time indicates the timeframe for an engineer to review the issue and respond with a technical plan.

Table 13.   Exclusions

	EXCLUSIONS
1	Non-production instances, including but not limited to testing, disaster recovery, training, or development.
2	Services, programs, enabling software or agents running on third-party provided systems.
3	Breach of any material obligations under terms or use or acceptable use policy per service contract.
4	When an issue occurs outside of standard working hours (as defined for business level customers), the SLOs do not apply.
5	SLOs do not include CCS offerings.
6	When resolution delay is due to lack of client response and/or customer provided credential based information.
7	Issues relating to customer internet access and/or customer content.
8	Any problems arising from customer or third-party provided software, hardware, technology, or equipment.
9	The priority levels are agreed upon by both customer and supplier.
10	Claims of performance degradation must be substantiated through customer provided diagnostic testing results.

TECHNICAL RESPONSE BY SERVICE LEVELS

Table 14. Incident Priority Definition Matrix

SERVICE	STANDARD	BUSINESS	ENTERPRISE
Monitoring	24x7x365	24x7x365	24x7x365
Notification			
Responses to Service Requests	Not included	Monday-Friday, 8 AM EST-5 PM EST	Monday-Friday, 8 AM EST-6 PM EST
Responses to Incidents			24x7x365
Notes	Virtustream can provide access to an engineer at a T&M basis during normal business hours, Monday-Friday, 8 AM EST-5 PM EST.	After hours support is not included and hourly support rates will apply. Overnight support requires a ticket, along with escalation from an authorized user by phone to the Service Desk. Any emails or XOC tickets sent after normal business hours without a call to the Service Desk for escalation by an authorized user will be handled on the next business day.	Full support, and overnight monitoring and emergency support as needed. Overnight support requires a ticket, along with escalation from an authorized representative by phone to the Service Desk. Any emails or XOC tickets sent after normal business hours without a call to the Service Desk for escalation by an authorized user will be handled on the next business day.

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.

EMC Response: We will have one lead one 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.

EMC Response: Virtustream provides 24/7/365 Support Center (xOC) via email or phone support.

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

EMC Response: Virtustream response times for acknowledgement and technical response and resolution are outlined within the attached addendum. All tickets are acknowledged within a business day. The technical response may vary depending on the priority level assigned at creation. Example a P1 has significantly different response cycles compared to a P4.

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

EMC Response: Virtustream will provide detail design of the solution, as required by Participating Entities.

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

EMC Response: Virtustream provides installation services, as self-service (all done by the customer), as shared-service (shared between Virtustream and Customer) and as Virtustream led (led by Virtustream and supported by the customer); in addition, Virtustream provides project based installation services.

IaaS Onboarding - Virtustream Led (IC-ONB-VLED-1T)

Virtustream will be responsible for provisioning the Virtustream IaaS Platform resources, project management, system migration, and environment architecture. Customer will provide information and support as required. All application installation, troubleshooting, and configuration are Customer's responsibility unless specifically contracted and scoped to be the responsibility of Virtustream personnel in the applicable Order Form.

If the Virtustream services provided include Two-Factor Authentication (2FA), then Onboarding includes issuance of two 2FA tokens.

Billing - One-time charge, per VM.

Table 15.   Onboarding Responsibilities, Virtustream Led

PLATFORM MIGRATION AND PRODUCTION READINESS		
TASK		
Define scope of engagement.	R	R
Provide detailed requirements for VMs and/or source files.	R	S
Project management / coordination.	C	R
Create client network(s), connections and firewall contexts.	C	R
Provision cloud resources, including compute, Storage, and xStream.	C	R
Create templates for new VMs or VMs from source files.	C	R
Setup basic monitoring.	C	R
Migrate data / VM source files for testing.	S	R
Install / configure applications and application connectivity.	R	S
Replicate data for production cutover.	S	R
Execute technical cutover (final data / networking).	S	R
Troubleshoot application issues.	R	S
Workload planning and stress testing (if applicable).	R	S

RASCI Definition:

- **R:** Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
- **A:** Accountable is the authority that approves the work of "R" before it is effective.
- **S:** Support "R" as necessary to complete the task or deliverable.

- **C:** Consulted reviews output or progress necessary to complete the task or deliverable.
- **I:** Informed needs to be notified of results, completion, or deliverable but need not necessarily consulted.

NOTE: When Virtustream is In the Support role or Consulted, Virtustream may charge Customer T&M for resources used.

IaaS Onboarding - Shared (IC-ONB-SHD-1T)

Virtustream will be responsible for enabling secure connection to our IaaS cloud and the provisioning of necessary our resources. All other roles and responsibilities will be determined and agreed upon at the time of project kickoff between Customer's technical resources and Virtustream onboarding resources.

Billing - One-time charge, per VM.

Table 16.   Onboarding Responsibilities, Shared

PLATFORM MIGRATION AND PRODUCTION READINESS		
TASK	CUSTOMER	VIRTUSTREAM
Define scope of engagement.	R	R
Provide detailed requirements for VMs and/or source files.	R	S
Project management / coordination.	R	C
Create client network(s), connections and firewall contexts.	C	R
Provision cloud resources, including compute, Storage, and xStream.	C	R
Create templates for new VMs or VMs from source files.	C	R
Setup basic monitoring.	C	R
Migrate data / VM source files for testing.	R	S
Install / configure applications and application connectivity.	R	S
Replicate data for production cutover.	R	S
Execute technical cutover (final data / networking).	R	S
Troubleshoot application issues.	R	S
Workload planning and stress testing (if applicable).	R	S

RASCI Definition:

- **R:** Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
- **A:** Accountable is the authority that approves the work of "R" before it is effective.
- **S:** Support "R" as necessary to complete the task or deliverable.
- **C:** Consulted reviews output or progress necessary to complete the task or deliverable.
- **I:** Informed needs to be notified of results, completion, or deliverable but need not necessarily consulted.

NOTE: When Virtustream is In the Support role or Consulted, Virtustream may charge Customer T&M for resources used.

IaaS Onboarding - Self Service (IC-ONB-SS-1T)

Virtustream will enable secure access to our IaaS Platform and will provision the resources detailed in the applicable Order Form on our Cloud Platform. A training session covering the xStream Portal will be scheduled by our team, approved by Customer and delivered by Virtustream. After training is completed a Customer can create new machines or upload existing machines to our IaaS Platform independently. VM creation, data transfer, and cutover operations are solely the responsibility of Customer.

The parties' responsibilities in connection with self-service onboarding process are summarized in the table below. In addition, Virtustream will assist in provisioning the environment and provide support where needed in transferring Customer data to the xStream Platform and offer best practice advice.

Billing - One-time charge, per account.

Table 17.   Onboarding Responsibilities, Self Service

PLATFORM MIGRATION AND PRODUCTION READINESS		
TASK	CUSTOMER	VIRTUSTREAM
Define scope of engagement.	R	C
Provide detailed requirements for VMs and/or source files.	R	C
Project management / coordination.	R	C
Create client network(s), connections and firewall contexts.	C	R
Procure, deploy, and monitor the connection between Customer and Virtustream's data center. This comprises managing the routers on each end as well as the circuit.	R	C
Provision cloud resources, including compute, Storage, and xStream.	C	R
Create templates for new VMs or VMs from source files.	C	R
Setup basic monitoring.	C	R
Migrate data/VM source files for testing.	R	S
Install / configure applications and application connectivity.	R	
Replicate data for production cutover.	R	S
Execute technical cutover (final data / networking).	R	S
Troubleshoot application issues.	R	C
Workload planning and stress testing (if applicable).	R	S

RASCI Definition:

- **R:** Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
- **A:** Accountable is the authority that approves the work of "R" before it is effective.
- **S:** Support "R" as necessary to complete the task or deliverable.
- **C:** Consulted reviews output or progress necessary to complete the task or deliverable.

- **I:** Informed needs to be notified of results, completion, or deliverable but need not necessarily consulted.

NOTE: When Virtustream is In the Support role or Consulted, Virtustream may charge Customer T&M for resources used.

IaaS Onboarding - Project Based (IC-ONB-PROJ-1T)

Virtustream will be responsible for enabling secure connection to our IaaS cloud and the provisioning of necessary team resources. All other roles and responsibilities will be determined and agreed upon at the time of project kickoff between Customer's technical resources and Virtustream onboarding resources.

Billing - One-time charge, per agreed upon onboarding services based on Customer requirements.

IaaS Migration Support (IaaS Onboarding Charge) - Project Based (IC- MIG-PROJ-1T)

Based on Customer input, Virtustream will assess Customer's migration needs, define a plan and schedule, and execute against the plan.

Billing - One-time charge based on Virtustream assessment of Customer requirements.

Security of Information

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.

EMC Response: Virtustream offers encryption services to protect customer data. Encryption: (All encryption technologies are FIPS 140-2 Certified)

1. In transit: IPSEC using AES256 Bit encryption
2. At rest: Vormetric using AES256 bit encryption
3. In archive: 128bit encryption
4. VM Host Image Protection and Encryption using SafeNet and AES256 bit encryption

Encryption keys are maintained in a HSM and access to the HSM requires multiple employees to administer to eliminate single administration risk issues. Encryption keys can be provided to the client using an encryption key wrapper and using a hand delivered physical security protocol.

Archive Data never leaves our owned infrastructure. Backup facilities are both located in CONUS. Backups are encrypted using FIPS 140-2 certified encryption and are stored locally on-site. Backups are replicated to another Virtustream CONUS location and use encrypted WAN connectivity to ensure that encryption is maintained throughout their lifecycle. Virtustream requires two-factor authentication to connect to the xStream management portal. Access to client applications is managed by client corporate authentication process, i.e., Active Directory.

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

EMC Response: Offeror implements reasonable and appropriate administrative/organizational, technical and physical measures to provide safeguards to comply with applicable laws and related to data privacy and security. Offeror will review laws and regulations identified in a Participating Addendum and applicable to Offeror. In addition, Purchasing Entities are required to encrypt data submitted to the Infrastructure as a Service (IaaS) or, alternatively, a Purchasing Entity can retain Offeror to encrypt the data. Encryption of data in transit must be configured on the transport layer with TLS to enable IaaS security controls to protect Purchasing Entity data at the IaaS in the Purchasing Entity zone.

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.

EMC Response: Offeror will not have access to Purchasing Entity's environment. Therefore, logical access to user accounts and data is not possible. Access to Purchasing Entity's data is only accessible as provisioned by the Purchasing Entity to specific Offeror personnel as part of a managed services contract. If needed for the specific service contracted by the Purchasing Entity, the Purchasing Entity will provide access to specific named Offeror personnel to perform the contracted tasks. Offeror personnel who are allowed access to Purchasing Entity's environments shall abide by Purchasing Entity's acceptable use policy for actions taken within their environment on their behalf. Each Purchasing Entity should invoke role-based access control to their systems.

Privacy and Security

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.

EMC Response: The Virtustream Federal Cloud (IaaS) has met the requirements for a FedRAMP moderate P-ATO. The IAAS is assessed annually by a FedRAMP certified 3rd Party Assessment Organization (3PAO). The annual assessment will review a subset of the NIST 800-53 Revision 4 controls as designated by FedRAMP. Virtustream's 3PAO shall demonstrate impartiality throughout the assessment to accurately assess the status of all security controls in place.

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.

EMC Response: Security is the foundation of our business. Our xStream™ cloud software assists our customers to meet mandatory Legislative requirements, and achieve and maintain SSAE16, ISAE3402, PCI-DSS 3.0, FISMA, IS0 27001-2005/2013, ISO 9001-2008, HIPAA, CSA STAR and other leading cloud certifications and compliance frameworks in the customer's own environment (when coupled with identified operational and management controls).

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.

EMC Response: All data for this environment will remain in the United States. Customers can elect Intel's TxT technology to demonstrate geo-fencing of data to specific data centers.

Virtustream data centers are physically accessible by designated employees and approved employees only. Virtustream employees who are assigned to the data center are issued a proximity card which is required to access the data center. Once inside, physical access to the data processing area is restricted to specific employees. Physical access to the data processing areas is protected by biometric locks on the doors. Data center personnel maintain a list of all approved personnel who have access to the data center offices and who have access to the data processing areas.

We offer security solutions which customers can select to protect their data while in transit and at rest. Customers are responsible for the protection of their data within their customer zone. Virtustream does not process, store, or disseminate customer data within the Virtustream-controlled management zone.

Virtustream invokes a defense-in-depth model for monitoring the management zone with tools such as Splunk, Trend Micro, Fortinet, and Tenable. These tools are available for customers to select as a managed service.

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).

EMC Response: Customers are responsible for the protection and confidentiality of data within their application and/or system which resides on the Virtustream IaaS. Virtustream customers are logically separated via VLAN and VRF technologies which ensure that different customers' data is not accessible and cannot be altered. Customers are responsible for controlling access to their data. Virtustream does not have direct access to customer data within their customer zone. Virtustream employees who are assigned to IaaS must pass a background investigation. In addition, Virtustream employees assigned to the IaaS must adhere to any requirement by customers to pass federal, state, or local background investigations if they are to provide managed services to the customer zone.

Virtustream offers an encryption at rest and encryption in transit managed service. This provides an additional level of protection for customer's data within their VLAN. All Virtustream employees with access to the IaaS are required to have hard drive encryption on their laptops. Our IaaS team performs quarterly privileged user access reviews.

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

EMC Response: Security is the foundation of our business. Virtustream's xStream™ cloud software assists our customers to meet mandatory Legislative requirements, and achieve and maintain FedRAMP, FISMA Moderate, PCI-DSS, SSAE16/SOC2/SOC3, ISO 27001/9001/22301, HIPAA, NIST 800-53, CSA STAR and other leading cloud certifications and compliance frameworks in the customer's own environment (when coupled with identified operational and management controls).

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.

EMC Response: Virtustream offers logging as a managed service to customers as optional solution. The types of services and devices are specified by the customer and a monthly report is delivered to the customer.

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

EMC Response: Virtustream does not have access to customer hosted data. Customers control access to their application or system which sits upon the IaaS. Customer would need to create the user in their own Active Directory to allow access by named users of Virtustream for specific system.

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.

EMC Response: Virtustream shall contact customers in accordance with Service Level Agreements (SLA) and contractual obligations.

There are two primary Incident types; Security Incidents, where there is a possible breach in systems or data integrity, and Services, where there is in impacted or affected service. Although there is some overlap, generally any security-related incident should be classified as a Security Incident and the response must be managed using the 'Virtustream Information Security Procedure – Security Incident Response Plan'.

The purpose of this security incident response plan is to provide general guidance to Virtustream staff- both technical and managerial – to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information including sensitive credit card data. The plan is also a guide to sharing information with other stakeholder organizations who might be impacted by such security incidents such as the credit card associations and law enforcement.

The Security Incident Response Plan (SIRP) provides guidance to prepare for, respond to, and recover from potential incidents. Policy statements surrounding the IR-Plan are provided to ensure continued upkeep and standardized use. The SIRP guidance at the procedural level defines the roles, responsibilities, communication methods and flows, contact information, types of potential incidents, and immediate actions that are to be taken upon an incident's identification, and elaborates with subsequent recovery steps. Virtustream's Incident Response Policy requires the implementation and testing of a generalized plan that adheres to the International Standards Organization 27002 guidance for incident management and response, but meets specific requirements for compliance such as PCI-DSS.

The Plan covers the corporate environment associated with Virtustream's IT assets, the local IT resources and the IT resources at Virtustream's Data Center. It consists of a series of guidelines (Incident Response Guidelines or "IRG") that should generally be followed as appropriate for the circumstances as when a security incident occurs or as part of the ongoing maintenance of this plan.

As the incident progresses and has more impact (i.e. severity level increases), the escalation process will be used to engage appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. The Table below defines the escalation levels with the associated team involvement.

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.

EMC Response: Virtustream utilized a virtual local area network (VLAN) and virtual route forwarding (VRF) to logically segregate all customers in the IaaS environment. Every customer chooses their own IP Address range, as there is no ability to overlap IP Addresses between customers. In addition, every customer is logically separated with Firewall Context with their own rule, where by default everything is denied except specific rule.

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)

EMC Response: Virtustream Cloud Platform Security (for the Infrastructure-as-a-Service environment) is designed, built, and operated to provide highest level of infrastructure security available.

Proposed Participating Entities Security Architecture

Figure 16.   xStream Enterprise Architecture
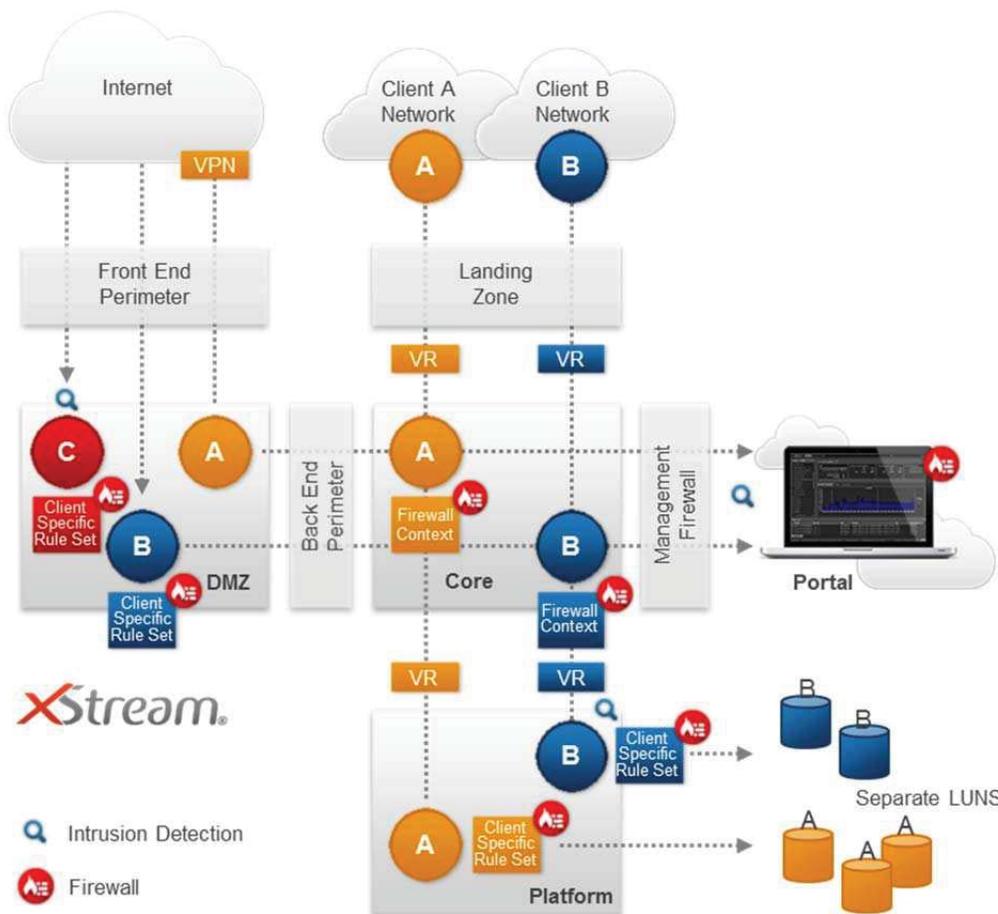
Participating Entities' end users would access the hosted environments via a MPLS connection (Provided by Participating Entities). Additionally a VPN connection has been sized at 100Mbps however this can be decreased or increased depending on the exact requirements.

Participating Entities' end users accessing our enterprise platform would first hit the landing zone in a dedicated virtual local area network (VLAN) and dedicated virtual route forwarding (VRF). The next hop into the enterprise platform is a dedicated firewall (FW) context on a Cisco Firewall services module. After traversing the core, traffic hits another dedicated VRF and drops into the platform network and compute (CPU and Memory essentially a blade server) layer. All traffic is VLAN separated. At each compute host, a hypervisor based firewall and intrusion protection system (IPS) provides a dedicated client rule set to further ensure network security. All traffic transitioning from one zone to another are monitored by Intrusion Detection and Intrusion Prevention systems.

Traffic coming in via the internet hits the front-end perimeter with load balancing modules and multi-context Cisco firewalls. All traffic then passes through intrusion detection system and intrusion protection systems. As in the enterprise compute layer, every host in our demilitarized zone (DMZ) has a hypervisor-based firewall and IPS with dedicated client rule sets. Again, all traffic is VLAN separated as well.

Traffic that needs to traverse from DMZ to the enterprise runs through another dedicated FW context and IDS/IPS. All of the Participating Entities' environments and data will be hosted in Virtustream's data centers within the continental United States. Standard Services used in Virtustream's management environment and in all client environments including the following:

- All Virtustream employees use Mandatory Strong 2 factor authentication (2FA OTP) Administrative Access to all systems.

- Dedicated VLAN network segmentation and dedicated Virtual Route Forwarding (VRF) are used extensively to segregate environments and zones.

- Perimeter Firewalls are used to segment internal and external environments as well as segregate security zones. Configuration, monitoring, auditing and logging are included.

- Virtual Machine-based Firewall and Intrusion Prevention System (IDS) is installed on every virtual machine in the environment and is protected with Juniper's Security Gateway virtual firewall application and monitored service.

Security Services that are standard components for Virtustream's management environment and are Optional Services for client environments including the following:

- Managed Two-Factor Authentication ("2FA") is in use for all application systems.

- Intel TxT Enabled Servers and Trusted Boot/Bios monitoring with Attestation Server and OS and VM support, including Geolocation and Geofencing according to NIST 7904 guidelines.

- Secure operating system (OS) builds based on DoD Secure Technology Implementation Guide (STIG) guidelines are used to build Virtustream's Management and Administration Servers.

- Server/File Integrity Monitoring (FIM) is installed in the PCI and VFC clouds.

- Patching Regimen: Virtustream patches host servers, network devices, security devices, servers and related services in the Management Network on a specified routine (monthly or quarterly, depending on release schedules), or when there is a CERT or other authorized source of patch that requires immediate attention. Based on urgency and risk of the issue we will schedule the patch as appropriate and use change control.

- Scanning regimen: vulnerability scanning is done on a monthly basis with additional 3rd party vulnerability scans done monthly. Additional scans are done when made aware of new vulnerabilities. Issues are classified and addressed according to Risk Classifications and are addressed with ITIL v3 change control processes.

- Managed IDS signatures are routinely updated and the logs are monitored.

- Anti-Virus is managed on all Management servers in Enterprise, PCI and, VFC clouds.

- Logging Service of all servers, network devices, and security devices to a centralized log server system.

- Governance Risk Compliance: We use a complete Enterprise Risk Management toolset to manage compliance reporting and continuous monitoring to all of our supported compliance frameworks.

Virtustream's facility monitoring systems are complete as per specifications in NIST 800-53r3/4. We use site assessment methodologies and checklists as detailed in NIST 800-42. Our systems and facilities are monitored 24/7 for any exceptions or trends. Our tools, processes and CONUS

(Continental USA) personnel monitor network, power, cooling, humidity, water leakage, fire suppression, power systems (utility power, UPS systems and generators) and site access.

Virtustream's Physical Access Control Security is designed to protect the confidentiality, integrity, and availability ("CIA") of the cloud platform system and its data with the following security components:

- Limited and controlled room access.
- Logged and monitored access of all access control events.
- Video surveillance and review of all access control events.
- Biometric access control required to gain access to the Data Center.
- US Data Center staff are limited only to US Citizens.
- Locked racks and rooms with key log out/in process.
- Data destruction policies and procedures.
- Asset in/out policy and procedures.

Physical access by authorized staff is controlled by badge systems and biometric access systems. All access of any kind is recorded and logged. Access lists are reviewed every 90 days. Employees that do not have a reason to have physical access are removed from our access management systems. Multiple high resolution and IR enhanced CCTV Cameras monitor our datacenters at all egress and ingress points as well as other sensitive areas. Security video footage is stored in a secure area for 90 days.

Approved Visitor Access requires VISITOR Badges and bright lanyards that are specifically different from employee badges. Visitors are required to produce and surrender a state or government issued photo ID during the visit, have a pre-approved reason for the visit, and have the escort witness the sign in and out procedure. Visitors are escorted continuously through approved areas of the facility. Visitors are not allowed access to following areas of the data center under any circumstances:

- Cloud hosting areas
- Networking and telecommunication areas
- Guard areas
- Power vaults

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.

EMC Response: Virtustream employees who are assigned to IaaS must pass a Virtustream background investigation. In addition, Virtustream employees assigned to the IaaS must adhere to any requirement by customers to pass federal, state, or local background investigations if they are to provide managed services to the customer zone which includes access to sensitive data.

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.

EMC Response: Virtustream's use of Intel® Trusted Execution Technology (Intel® TXT), a hardware-root of trust security feature, and Intel® AES-NI encryption acceleration helps secure and protect virtualized environments against malware and provides more of the critical infrastructure and data protection assurances needed to enable trusted multi-tenancy in the cloud. Our solution for data-at-rest and data-in-transit encryption requirements for our customers is optional service, as most of our customer environment is only accessible via private network and only to the internal users of the customer. Solutions available to our customer are:

1. IPSEC VPN Tunnel for data-in-transit and
2. VM level encryption for files and databases
3. Encrypted Backup (all backups are encrypted by default)

The technologies of encryption available throughout the entire data lifecycle and all are FIPS 140-2 compliant.

a) DB and File System Encryption

b) Encrypts file system and volume data transparently to:

      i) Applications

      ii) Databases

      iii) Storage Infrastructure

c) Integrated Key Management

d) High Efficiency Encryption

      i) Centralized Key Management

      ii) Policy Management

      iii) Detailed Auditing

      iv) Highly Available

      v) FIPS 140-2 Certified Hardware Appliance

      vi) Very Low Encryption Penalty due to Intel AES-NI enabled chip sets used

e) Encryption of Virtual Machine, OS and App

      i) Integration of SafeNET Protect-V

      ii) Logging of all image access

f) Encryption in Archive

g) Implements Encryption, Access Control, Auditing on Host (LUW)

h) Kernel Level Driver – Win

i) File System – Unix/Linux

j) Support for file systems and raw partitions

k) Highly efficient block encryption

Our IaaS offer will enable Participating Entities to select the level of security deemed appropriate to conform to their data risk profile.

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.

EMC Response: There are two primary Incident types; Security Incidents, where there is a possible breach in systems or data integrity, and Services, where there is in impacted or affected service. Although there is some overlap, generally any security-related incident should be classified as a Security Incident and the response must be managed using the 'Virtustream Information Security Procedure – Security Incident Response Plan'.

The purpose of this security incident response plan is to provide general guidance to Virtustream staff- both technical and managerial – to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information including sensitive credit card data. The plan is also a guide to sharing information with other stakeholder organizations who might be impacted by such security incidents such as the credit card associations and law enforcement.

The Security Incident Response Plan (SIRP) provides guidance to prepare for, respond to, and recover from potential incidents. Policy statements surrounding the IR-Plan are provided to ensure continued upkeep and standardized use. The SIRP guidance at the procedural level defines the roles, responsibilities, communication methods and flows, contact information, types of potential incidents, and immediate actions that are to be taken upon an incident's identification, and elaborates with subsequent recovery steps. Virtustream's Incident Response Policy requires the implementation and testing of a generalized plan that adheres to the International Standards Organization 27002 guidance for incident management and response, but meets specific requirements for compliance such as PCI-DSS.

The Plan covers the corporate environment associated with Virtustream's IT assets, the local IT resources and the IT resources at Virtustream's Data Center. It consists of a series of guidelines (Incident Response Guidelines or "IRG") that should generally be followed as appropriate for the circumstances as when a security incident occurs or as part of the ongoing maintenance of this plan.

As the incident progresses and has more of an impact (i.e. severity level increases), the escalation process will be used to engage the appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. The Table below defines the escalation levels with the associated team involvement.

Migration and Redeployment Plan

8.7 (E) MIGRATION AND REDEPLOYMENT PLAN

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

EMC Response: Virtustream provides secured data removal based on contractual obligation. If there is a data retention period, Virtustream will work with the Purchasing Entity to ensure compliance.

Virtustream has specific process for the removal of data and media, as described below. The process will be carried out by operations staff and validated by Security Operations.

Magnetic Media

All magnetic and optical media (CD's, Tapes and Floppy disks) that are deemed bad or are not needed post contract dates will be physically destroyed and where necessary logged via xOC ticket system and ISF-07 Equipment Disposal Form.

Hardcopy Information

The Company provides document-shredding equipment. Where deemed necessary all employees are aware that they are require to shred 'confidential and other information' that may be considered by the employee as sensitive.

Storage Equipment

Storage equipment / media is erased or physically destroyed.

Where possible information stored on flash memory devices is overwritten and this includes all pen drives and system cards that store information in flash memory, if not in use.

Cardholder, PII, PHI, Customer Proprietary data

Where data or secure systems data may be present on electronic media, this media will be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing, crushing).

Customer Data De-Provisioning

After securely returning data to client any data that remains after a customer POC or contract comes to termination; all data will be located and destroyed so as to be rendered irretrievable. The disk repetitive overwrite process will be used as described by NIST 800- 88 Rev.1. This is applicable to Laptops used to process customer data as well.

Secure Wipe Process with Vendor Specific Storage Array

Virtustream deploys vendor specific technology adhering to the contractual obligation and Virtustream's internal policy for data destruction.

Encryption Key Destruction Method

For clients that are using encryption, the most secure and expedient way to eliminate access to data is to destroy the encryption key, thus rendering the data unusable. Our Managed Encryption Service offers this during de-provisioning process with a secure and auditable process. Our Backup systems offer a similar process to shred keys. Please refer to the appropriate operational guide.

Inoperable Hard Drives

Will be removed from the server or storage array. All the hard drives or bad media that are bad will be marked and stored in a box located in the OCC marked for destruction. Only Data Center Staff and Security have access to that room. No sales or other employees have access without being escorted.

After a bad HDD or Media drive leaves the data center, it will be tagged by us and scanned by the destruction company for us to follow a secure path to destruction followed by a certificate of destruction.

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.

EMC Response: Virtustream offers Anti-Virus protection based on per virtual machine, per month charge.

Service or Data Recovery

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.

EMC Response: In the event of extended downtime affecting production systems, Virtustream and customer would jointly evaluate the situation and mutually decide on to declare a failover declaration. Then our team would then execute the failover plan to restore customer operations to the secondary data center maintain communication with the Participating Entity affected.

b. Suffers an unrecoverable loss of data.

EMC Response: Multiple copies of customer data exist in multiple datacenters – in the primary datacenter, there is the production copy and a local backup. The local backup is replicated to a secondary datacenter and the production datastores associated with core VM's are also replicated at regular intervals to the secondary datacenter. If a Participating Entity feels that additional steps/redundancy are required to maintain recoverability, we can work with the Participating Entity to find a solution.

c. Offeror experiences a system failure.

EMC Response: Virtustream has built redundancy into all layers of the physical infrastructure in order to deliver SLAs up to 99.999% and mitigate the risks of a system failure. Additional levels of protection include regular system backups (stored locally and replicated offsite) as well as automatic storage replication to a secondary data center to facilitate the ability to restore operations in the event of a system failure.

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

EMC Response: Basic Plus µVM's are designed for mission-critical workloads and for systems that require DR, addition of reserved compute capacity in a secondary datacenter (i.e. Reserve µVM) and automatic storage replication to facilitate the ability to restore operations in the event of an outage at the primary data center. RPO and RTO for core µVM's are 15 minutes and 2 hours respectively.

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

EMC Response: Virtustream's solution will have a Recovery Point Objective (RPO) of 2 Hours and Recovery Time Objective (RTO) of 30 Minutes for all disaster recovery enabled workloads.

The Virtustream Cloud has been designed to deliver continuous operations. The platform is architected to be highly available, with SLAs as up to 99.99%. All infrastructure systems are run in at least an N+1 model and have been designed with no single points of failure. All of the data center facilities and infrastructure has redundant power supplies connected to separate circuits from separate power feeds. Every device is connected via redundant pathways at a LAN/SAN/WAN layer.

Participating Entities can choose any of our FedRAMP Data Centers to host their applications and the DR location. For illustrative purposes, we have assumed the primary data center will be USDC02 and DR data center would be USDC01.

The Participating Entities' solution has been designed with all workloads running in our San Francisco (USDC02) data center. In the unlikely event of a disaster at the USDC02 facility, Participating Entities' production services will be brought back online in the secondary data center located in Northern Virginia (USDC01). The target RPO is 30 minutes for virtual machines with a 2 hour RTO. All production workloads in the primary node will have reserved compute capacity in the secondary node when deployed using Reserve µVMs and replicated storage. All virtual machine disaster recovery services are based on storage replication. The primary and secondary data centers are interconnected by diverse private 10 Gbps Sonet rings from separate Tier 1 providers – AboveNet and Level 3. Data is replicated asynchronously and continuously between the two data centers. Virtustream also performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by Participating Entities per landscape and will be documented during the on-boarding process.

Figure 17.   Integrated Disaster Recovery

Virtustream's cloud platform includes integrated disaster recovery (30 Min RPO & 2 Hr RTO) and backup.
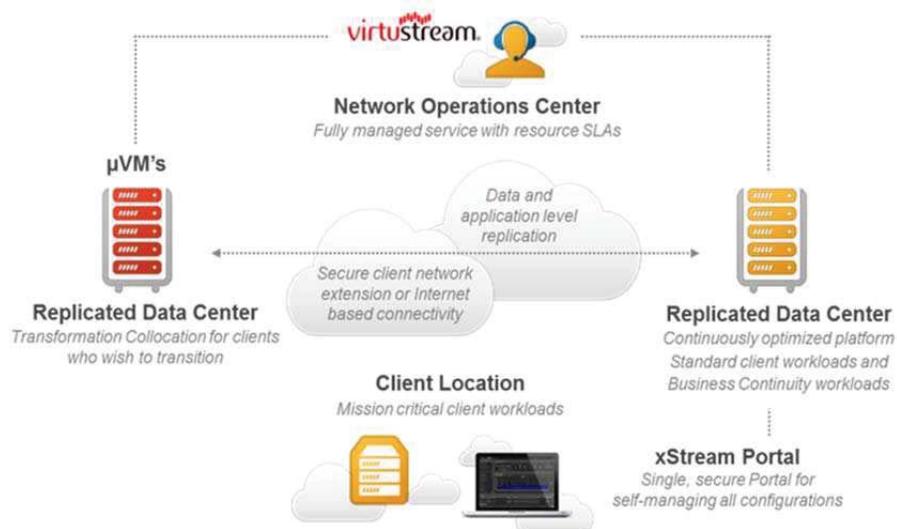
8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups

EMC Response: Virtustream performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by Participating Entities per landscape and will be documented during the on-boarding process.

Virtustream provides OS level files are protected with a File System backup and then protect the application with an integrated solution. Some of the databases would dump to a flat file format and those files would be protected with the standard file system backup.

b. Method of server image backups

EMC Response: OS level files are protected with a File System backup and then protect the application with an integrated solution where available. Otherwise databases would dump to a flat file format and those files would be protected with the standard file system backup. Additionally, core μVM's are automatically replicated to a secondary datacenter for DR purposes.

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

EMC Response: Virtustream performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by Participating Entities per landscape and will be documented during the on-boarding process.

Backup data is stored on local enterprise class disk storage systems and can be replicated to systems in a secondary Virtustream datacenter. All of Virtustream backup is disk based solution.

Encryption keys are generated at the time of backup application install on the Client VM(s). Encryption keys are at least AES-128 but can be AES-256. Keys are stored on the backup system databases using the encryption key management tool, the data about the keys on the database is in a unreadable format and cannot be decrypted.

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

United States.

EMC Response: Participating Entities can choose any of our FedRAMP Data Centers to host their applications and the DR location. For illustrative purposes, we have assumed the primary data center will be USDC02 and DR data center would be USDC01.

The Participating Entities' solution has been designed with all workloads running in our San Francisco (USDC02) data center. In the unlikely event of a disaster at the USDC02 facility, Participating Entities' production services will be brought back online in the secondary data center located in Northern Virginia (USDC01). The target Recovery Point Objective (RPO) is 30 minutes for virtual machines with a 2 hour Recovery Time Objective (RTO). All production workloads in the primary node will have reserved compute capacity in the secondary node when deployed using Enterprise Reserve µVMs and replicated storage. All virtual machine disaster recovery services are based on storage replication. The primary and secondary data centers are interconnected by diverse private 10 Gbps Sonet rings from separate Tier 1 providers – AboveNet and Level 3. Data is replicated asynchronously and continuously between the two data centers. Virtustream also performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by Participating Entities per landscape and will be documented during the on-boarding process.

Data Protection

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.

EMC Response: At rest encryption is enabled on both the Avamar Virtual Edition (AVE) and Data Domain devices. The AVE at rest encryption is 256AES CFB and the Data Domain is 256AES GCM allowing for the best available encryption while balancing optimal performance. AVE inflight encryption is specified at the highest available setting allowing for 256AES GCM and the strongest associated OpenSSL suites supported by the backup clients. Encryption key management is handled internally by the individual instances of AVE and Data Domain systems.

Virtustream offers two types of encryption techniques:

Software-based Encryption - The Backup Session Manager (BSM) reads the backup specification in which the AES 256-bit encryption option is selected and requests an active encryption key from the Key Management Server (KMS). The key is transferred to the Disk Agent (Client), which encrypts the data. Thus the backed up data is encrypted before it is transferred over the network and written to media.

Drive-based Encryption - The BSM reads the backup specification in which the Drive-based encryption option is selected and requests an active encryption key from the KMS. The key is transferred to the Media Agent (MA), which configures the drive for encryption and sets the encryption key into the drive. The drive encrypts both the data and the meta-data that is written to the medium.

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.

EMC Response: To the degree EMC is a "business associate" under HIPAA, EMC is willing to negotiate in good faith and enter into an applicable Business Associate Agreement or any other agreement that EMC and the Purchasing Entity agree are applicable and necessary to protect data of the 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.

EMC Response: Virtustream does not have access nor do we mine customer data.

Service Level Agreements

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.

EMC Response: Virtustream's Service Level Agreement is generally not negotiable. Our SLAs are one of the strictest in the market place. To change the SLA would mean either changing the design or create operational disruption and higher cost by engaging in non-standard processes and practices. For example, Virtustream's SLA for Tier 1 storage is 10 ms latency. For Virtustream to change this latency means changing the design for Tier 1 storage.

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.

EMC Response: Below is a sample of Virtustream's Service Level Agreement:

Service Level Framework

The service levels ("Service Levels") applicable to the Services specified in Sections 1 and 2 are set forth in Schedule B to this SD ("Service Levels for Cloud Platform Services"). The framework that governs all Service Levels is set forth in this Section.

Commencement of Service Levels

Commencing thirty (30) days from the Service Start Date (as set forth in the applicable Order Form), Virtustream's performance of the Services will meet each applicable Service Level. If Virtustream's performance of the Services does not meet the applicable Service Level, then Virtustream will use commercially reasonable efforts to restore its performance to meet such Service Level.

Service Level Reports

Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month,

broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all our customers use CPS.

Service Level Review Meetings

Monthly Service Level review meetings will be conducted by our team with the Participating Entity where the monthly Service Level report specified above will be discussed. If any of the Service Levels measured over the previous calendar month period is not achieved in that month, then Virtustream will include the steps taken to rectify the problem in the next monthly Service Level Report. In addition, the issue shall be an agenda topic for discussion at the next monthly service review meeting. Additionally, after restoring service or otherwise resolving any immediate problem as specified in this SD, if Virtustream fails to provide Services in accordance with the Service Levels, Virtustream shall:

a. Promptly investigate and report on the causes of such problem.

b. Provide a Root Cause Analysis of such failure as soon as practical after such failure or at Customer's request.

c. Correct such problem that is Virtustream's fault or responsibility, as soon as reasonably practicable and coordinate the correction of such problem if Virtustream does not have responsibility for the cause of such problem.

d. Advise Customer of the status of remedial efforts being undertaken with respect to such problem.

e. Demonstrate to Customer's reasonable satisfaction that the causes of such problem (that is Virtustream's fault or responsibility) have been or shall be corrected on a permanent basis.

f. Take corrective actions to prevent any recurrence of such problem (that is Virtustream's fault or responsibility).

Root Cause Analysis

Promptly following Virtustream's failure to meet a Service Level, Virtustream will perform a root cause analysis to determine the reason for that failure. Upon Virtustream's determination of the cause of such failure, it will provide to Customer a preliminary report citing the cause of such failure. If Virtustream determines that the failure was due to Virtustream, an additional report will be provided that details the root causes of the failure, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. Virtustream will correct the problem and use reasonable commercial efforts to minimize the re-occurrence of such failures.

Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels; to the extent such failure was caused by one or more of the following:

a. A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD.

b. Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer).

c. Any hardware, software or other product of a third-party or Customer equipment.

d. Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility.

e. Downtimes resulting from a Virtustream's scheduled maintenance windows.

f. Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level.

g. Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date.

h. An election by Customer to purchase a base commitment that is not sufficient to run Customer's system (e.g., If a customer elects to size a µVM pool that is insufficient to run the designated workload).

i. Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply.

j. Cloud Cover Services (CCS) offerings — for which the Service Level Objectives (SLOs) do not apply.

k. Resolution delays due to lack of client response and/or Customer provided credential based information.

l. Priority levels not agreed upon by both customer and supplier.

m. Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

Data Disposal

8.11 (E) DATA DISPOSAL

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

EMC Response: Secure wipes are accomplished through a utility called Disk Sanitization. This license is permanent and enables the disk sanitize command and limited SnapMirror replication abilities that facilitate selective sanitization operations. The obliteration is accomplished by means of overwriting the entire disk with user defined patterns of data, multiple times. The disk sanitize feature performs a disk format operation and uses three successive byte overwrite patterns per cycle and a default six cycles per operation for a total of 18 complete disk overwrite passes, in compliance with United States Department of Defense and Department of Energy security requirements.

Disk sanitization is performed on one or more physical disk drives. Users can sanitize or cleanse all disks associated with a complete WAFL volume (and spares) or perform sub volume cleansing such as cleansing a tree, a directory, or file. If sub-volume cleansing is desired, all data that should remain in physical volume after cleansing must be migrated to another volume on the same storage appliance or another storage appliance prior to the start of the cleansing process. The limited SnapMirror abilities enabled are used to assist in data migration if you migrate to another volume on the same appliance. Once the data migration is complete, sanitization can be performed on all the drives associated with the initial volume.

Performance Measures and Reporting

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.

EMC Response: Our solution for VM workload includes the uptime of 99.99%.

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

EMC Response: Virtustream IaaS Compute is comprised of computing resources hosted in secure data centers that replace the physical computing hardware traditionally housed on Customer site. These resources include physical servers which are logically divided into VMs (virtual machines), each with an allocation of CPU and memory, and linked to storage.

Terms used in the detailed descriptions below:

- **μVM.** Pronounced "micro VM," this is Virtustream's fine-grained unit of measurement designed to accurately measure the actual consumption of cloud resources. A μVM is a unit of computing resources, comprised of CPU, memory, storage IOPS, and associated local network bandwidth.

  The usage of each μVM resource component (CPU, memory, storage input/output, and network bandwidth) is measured at five minute intervals — one unit each for 200MHz of CPU, 768MiB of memory, 40 storage fabric input/output operations per second (IOPS), and 2Mbps of local network bandwidth. The highest of the four is averaged per hour, and the hour values averaged across the month to determine the overall μVM usage for the month.

  Note: The measurement is performed at the aggregate level — across Customer's entire μVM resource pool. Bandwidth usage is only within the data center.

- **Basic Plus μVM.** These terms differentiate the two ways Virtustream offers μVMs services.

  "Basic Plus" μVM services are limited to a single Virtustream data center and have 99.99% availability for the Customer's committed level.

  "Reserve" μVM service is an equivalent quantity of Basic Plus μVMs reserved at Customer-designated secondary Virtustream data center for on-going operation during disaster events and during scheduled disaster recovery (DR) exercises.

  In both cases, overage resources required ("surges") up to 20% above the committed level from the contract /order form is provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

- **High Memory.** Virtustream offers competitive pricing on compute services for applications that require large amounts of memory (64GiB or more).

- **Enterprise** These terms identify the "zones" within which μVMs are made available for consumption. The "Enterprise" zone is for use by non-Internet facing workloads. Systems deployed into the Enterprise zone are not directly accessible from the Internet.

Enterprise Basic Plus µVM (IC-µVM-BASP-ENT)

Enterprise Basic Plus µVMs reside in a single Virtustream data center, in the Enterprise zone. Resource availability is 99.99%, and only at the designated data center.

Overage resources required ("surges") up to 20% above the committed level from the contract /order form is provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

Service Level - 99.99% availability for the Customer's committed level.

Billing - Monthly, based on resource usage.

Tier 0 Block Storage - Local Only (IC-STO-TOA-LOC)

Block storage with a Latency Service Level of 3ms that is maintained in a single data center with no replication capability.

Billing - Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

Tier I Block Storage - Local Only (IC-STO-T1A-LOC)

Block storage with a Latency Service Level of 10ms that is maintained in a single data center with no replication capability.

Billing - Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

Tier II Block Storage - Local Only (IC-STO-T2A-LOC)

Block storage with a Latency Service Level of 20ms that is maintained in a single data center with no replication capability.

Billing - Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

Tier III Block Storage - Local Only (IC-STO-T3A-LOC)

Block storage with a Latency Service Level Objective of 40ms that is maintained in a single data center with no replication capability.

Billing - Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

Tier 0 Block Storage - Replicated (IC-STO-TOA-REP)

Data storage with a Latency Service Level of 3ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level - Recovery Time Objective (RTO) of four (4) hours, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing - Monthly fee, based per GB of storage allocated.

Tier I Block Storage - Replicated (IC-STO-T1A-REP)

Data storage with a Latency Service Level of 10ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level - Recovery Time Objective (RTO) of four (4) hours, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing - Monthly fee, based per GB of storage allocated.

Tier II Block Storage - Replicated (IC-STO-T2A-REP)

Data storage with a Latency Service Level of 20ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level - Recovery Time Objective (RTO) of four (4) hours, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing - Monthly fee, based per GB of storage allocated.

Tier III Block Storage - Replicated (IC-STO-T3A-REP)

Data storage with a Latency Service Level Objective of 40ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level - Recovery Time Objective (RTO) of four (4) hours, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing - Monthly fee, based per GB of storage allocated.

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.

EMC Response: Virtustream will work collaboratively with Participating Entities to develop / maintain a relationship structure that leads to quick resolution, regularly scheduled status meetings, and quarterly business reviews.

Virtustream will assign multiple key personnel to Participating Entities including an Executive level sponsor. The primary point of contact will be Virtustream's Technical Account Manager (TAM). The TAM is responsible for daily activities/interaction and understanding/ensuring Participating Entities' objectives are met at a minimum. Optimizations and other improvements to processes/standard operating procedures are delivered by the TAM in coordination with other Virtustream staff working behind the scenes. The TAM will coordinate day-to-day operation, service level management and SL reporting.

The following outlines Virtustream's approach to service desk escalation and issue resolution.

Escalations within Virtustream

Virtustream will provide Level 0 and Level I support and first call resolution where possible, as determined by Virtustream. Where first call resolution is not possible, the Virtustream Service Desk provides incident management for Incidents and Urgent Service Requests escalated to Level II and Level III resources as defined below.

In the event that Virtustream's Response to an Incident is not acceptable to the Customer, Customer can contact our Service Desk and request escalation to the head of the Service Desk. Virtustream shall, upon receipt of any such request, immediately escalate the issue to the head of the Service Desk or technical team as appropriate.

Service Request Prioritization

Service Requests are assigned a priority of either 'Urgent' or 'Standard' and are queued for fulfillment with the corresponding priority. All Service Requests will be reviewed by the Virtustream Service Desk, who will determine the appropriate priority to assign with collaboration of Customer.

Incident Prioritization

All Incidents that are reported to the Virtustream Service Desk or that Virtustream otherwise becomes aware of, will be initially assigned a priority by the Virtustream Service Desk as set forth below. Internal escalation for Incidents to Level II and Level III resources are based on the priority level assigned to the Incident.

Table 18.   Incident Prioritization

INCIDENT PRIORITIZATION			
PRIORITY/ SEVERITY	**DEFINITION**	**RESPONSE TIME SERVICE LEVEL**	
1	Major part of the system is unavailable/not operating correctly, affecting multiple users. No workarounds in place and business operations are not possible. **Or** Incident has a critical impact on the business (e.g., loss of the Exchange Production server impacting all users).	**30 minutes**	Response time will be within indicated time beginning from when the customer creates a ticket or a monitoring event is validated. Additional resources are engaged via Virtustream's on Call Process.
2	Part of the system is unavailable/not operating correctly, affecting users in a single function. No workarounds in place and business operations in this function are not possible/severely impacted. **Or** Incident has a serious impact on part of the business (e.g., a configuration change is impacting a small subset of users).	**60 minutes**	
3	Part of the system is unavailable/not operating correctly, affecting users in a single function. Workarounds in place, but business operations are impacted, although not severely. **Or** Incident has a temporary impact on users and is non critical or is a development issue (e.g., email is slow to deliver)	**4 hours**	
4	Incident that is causing inconvenience to the business, but not impacting operations. **Or** Incident has a minor impact on users or business, or issue is a request for further information	**1 business day**	

Virtustream will assign a Technical Account Manager starting on day 1 of the contract. The Cloud Platform, Cloud Cover (managed services), and Cloud Security team's will also be assigned to Participating Entities upon execution of the contract. All of the individuals assigned to the Participating Entities account have significant years of experience in their fields.

The TAM assigned to a Participating Entity can provide ad hoc reports but will provide reports on a quarterly basis. The quarterly business reviews include but are not limited to performance measurements, service requests. On a monthly basis, the TAM will provide a consumption report detailing the items consumed by each virtual machine. This delivers a very granular cost breakdown to Participating Entities which will allow the data to be carved multiple ways. Also, information can be gathered by the Participating Entity's team any time they want from the xStream portal. Participating Entities can also issue a ticket to Virtustream operations center to request information as well. The TAM will conduct scheduled meetings and be in constant contact with Participating Entities. The TAM is an extension of the Participating Entity's team.

Virtustream defines a Root cause analysis (RCA) as the formal process, documented in writing by Virtustream and approved by Customer, to be used by Virtustream to diagnose problems at the lowest reasonable level which includes a report of the corrective action to be taken and defined timelines for corrective actions, which shall eliminate, to the extent reasonably possible, repeat failures. The following details the RASCI for RCAs:

Table 19.   RASCI for RCAs

ROLE/FUNCTION	CUSTOMER	VIRTUSTREAM
Request Root Cause Analysis tickets by contacting the Virtustream TAM (Customer requests Incident report/Problem record)	R/A	S
Document, track and manage all Problem tickets using ITSM system	S	R/A
Provide Problem management review and Root Cause Analysis (RCA) for all in-scope P 1 Incidents (preliminary report within 48 hours; final within 15 calendar days)	S	R/A
Provide Problem management and RCA of identified Problems (e.g., reoccurring events, alerts) - investigate and diagnose	S	R/A

RASCI Definition:

- **R:** Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."

- **A:** Accountable is the authority that approves the work of "R" before it is effective.

- **S:** Support "R" as necessary to complete the task or deliverable.

- **C:** Consulted reviews output or progress necessary to complete the task or deliverable.

- **I:** Informed needs to be notified of results, completion, or deliverable but need not necessarily consulted.

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

EMC Response: Our TAM will collect on a monthly basis, the performance data on incident response and other service level elements and report to the customer. In case of Virtustream not meeting response times, the case will be investigated, findings presented, remediation plan developed and also presented during the monthly review. The implementation of the remediation plan will be tracked and presented monthly.

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

EMC Response: Planned downtimes start with the weekly change board meeting by the Platform Operations group. All requested changes whether requested by customers or by the operations staff are reviewed, if approved then scheduled. Depending on the nature of the change, routine and planned, the affected customers are notified as early as possible and adjusted based on customer needs. For example, if the scheduled downtime falls on a weekend that a customer plans to do their quarterly close, we will reschedule. An emergency/urgent change may have less notice for the customers. But in all cases, customers will be notified of the upcoming downtime on multiple occasions. Notification will include the start of the downtime and the expected duration. Once the downtime is complete, another notification will go out to the affected customers.

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

EMC Response: If the DR recovery metric is not met then availability SLA will not be met. Virtustream has a service credit schedule as shown below which will be used to provide service credits in case of prolonged outage resulting from slow DR activation.

Service Level Credit Structure

Virtustream will provide to Customer a Service Level Credit for any month in which Virtustream fails to meet the applicable Service Level (each such failure, a "Service Level Failure") as set forth below.

Table 20.   Service Level Credit Structure

µVM AVAILABILITY ON ENTERPRISE BASIC PLUS µVM	SERVICE LEVEL CREDIT*
>99.95% and <99.99%	1%
>99.9% - 99.95%	3%
95% - 99.9%	5%
90% - 94.99%	10%
Below 90%, or if, the µVMs specified in applicable Order Form are not Available for a consecutive 8 hour period.	15%

I.   Where a single Incident results in more than one Service Level Failure, Virtustream will provide Customer with only the largest Service Level Credit. Customer will not be entitled to Service Level Credits for each of such Service Level Failures.

II. Virtustream will credit any Service Level Credit against the charges otherwise payable by Customer to Virtustream, on the next invoice with respect thereto. If no further charges are due and owing to Virtustream, Virtustream shall pay Customer the applicable Service Level Credit within forty-five (45) calendar days of the date such credit was incurred.

III. If Customer's accounts receivable balance is not current in the month in which the Service Level Failure occurred (i.e. Customer has not paid its invoices in accordance with the terms of the MSA), Customer shall not be entitled to a Service Level Credit, and Virtustream will be excused for its failure to meet or exceed the Service Levels.

IV. In no event will the aggregate of all Service Level Credits paid under an Order Form in any month exceed fifteen percent (15%) of the total fees payable for such month pursuant to the applicable monthly invoice.

Service Level Exceptions:

Virtustream shall not be liable for any failure to meet the Service Levels; to the extent such failure was caused by one or more of the following:

a. A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

b. Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);

c. Any hardware, software or other product of a third-party or Customer equipment;

d. Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;

e. Downtimes resulting from a Virtustream's scheduled maintenance windows;

f. Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;

g. Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date;

h. An election by Customer to purchase a base commitment that is not sufficient to run Customer's system;

i. Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply;

j. Cloud Platform Services (CPS) offerings — for which the Service Level Objectives (SLOs) do not apply;

k. Resolution delays due to lack of client response and/or Customer provided credential based information;

l. Priority levels not agreed upon by both customer and supplier;

m. Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

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.

EMC Response: Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.

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

EMC Response: Through the xStream portal customers may generate reports on usage and other performance data on their workloads.

xStream portal integrates powerful Jasper reporting engine. A Detailed CSP Consumption Report provides μVM consumption information per VM for all the tenants. This report is only available to the service provider. EMC has provided an example CSP Consumption Report an attachment to the technical proposal titled "CSP Consumption BG Report-report.pdf".

Tenant Consumption Report, which provides μVM consumption data per each VM for the given tenant, is available to both, CSP and the tenant. xStream fronts consumption data for reporting for up to 3 months. Data goes into archive once it reaches 3 months age. All consumption data is stored in the xStream CMP Data Warehouse.

The DW is deployed as part of the xStream CMP management landscape and provides a series of materialized views for the Reports or direct querying of tenant consumption data by Cloud Service Provider users. The data uses PostgreSQL 9.4 and provides a series of materialized views which aggregate raw Performance Metric data archived as part of a nightly ETL job. Service provider can add additional Jasper reports to meet any specific needs.

Figure 18.   xStream Portal Example View
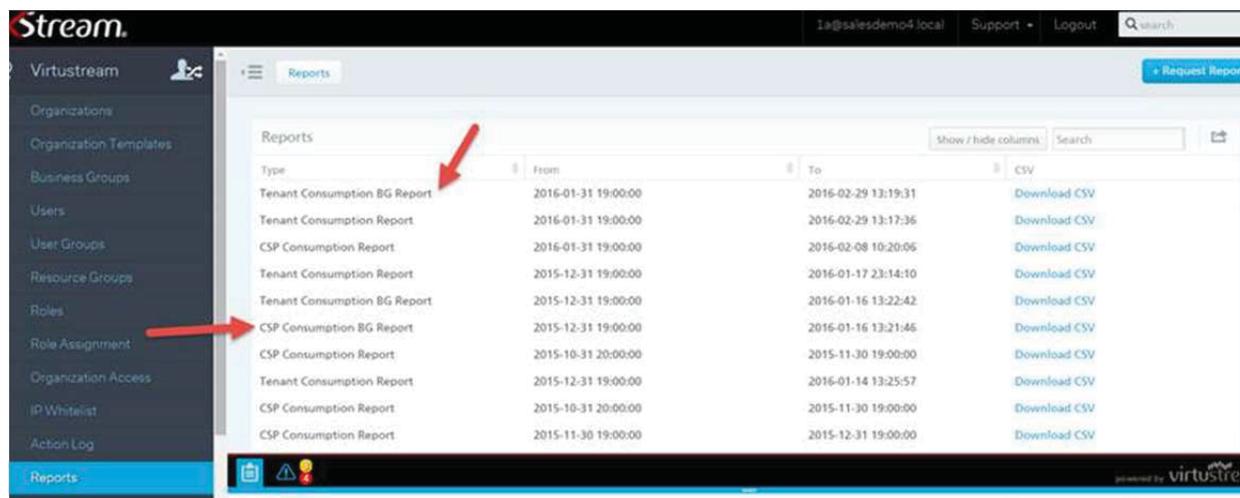
8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

EMC Response: Virtustream's self-service portal allows authorized users to deploy resources on-demand 24x365.

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

EMC Response: Virtustream's self-service portal allows authorized users to deploy or de-commission resources on-demand 24x365.

Cloud Security Alliance

8.13 (E) CLOUD SECURITY ALLIANCE

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

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

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

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

d. Completion CSA STAR Continuous Monitoring.

EMC Response: We maintain our CSA Audit online. As per the requirement guideline of the RFP response, Virtustream will be providing the CSA STAR CAIQ as an attachment.

Service Provisioning

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.

EMC Response: Customers have the ability to leverage Self-Service through the xStream Portal if needed whereby they can provision their own VMs if the need is urgent

Additionally, xStream supports Cloud Management Providers the capability to provision VM instances "on behalf of" a Purchasing Entity and our IMS Team can called to assist in an urgent situation to assist in such requests.

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

EMC Response: Virtustream's standard lead-time for provisioning can vary based of the type of deployment and requirement. Resources can be deployed on-demand basis by Participating Entities. For the initial services, there is a standard which is maintained as best practice.

At project kick-off, our team and a Participating Entity will develop a detailed Implementation Plan, on a system-by-system, week-by-week basis, to ensure that both sides of the relationship have clear expectations on what is to be accomplished, by whom, and in what timeframe. Upon completion of the Implementation Plan, our team and the Participating Entity will establish a Project Governance Plan and the Project Governance Plan will manage Implementation Plan and ensure alignment at all tiers of the organization, define expectations for status update frequency and formats, and establish an escalation path for issue identification and resolution.

We offer a dedicated onboarding project team that is charged with migrating clients into the xStream® cloud. This chargeable service includes resources from our platform and SAP teams and development of an onboarding project plan with milestones and deliverables. We use a

mature methodology to move clients onto our cloud platform, a process which is continuously refined and improved. A link is established to the client site using a Virtual Private Network (VPN) or Multiprotocol Label Switching (MPLS) circuit, for customer access and testing of migrated systems. Prerequisites are put into place (domain controllers, backup systems, infrastructure, networking, etc.) prior to systems being onboarded, in a defined sequence. Virtustream SAP basis team members test the systems before turning them over to Ascend for validation. Once on the xStream® platform, our team monitors, backups and maintains the systems. As a component of the IaaS platform, all core units are replicated to an alternate data center to provide disaster-recovery capability.

Figure 19.   Sample Work Plan

Back Up and Disaster Plan

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.

EMC Response: Specific retention requirements can be accommodated on a custom basis. More detailed information would need to be provided in order to scope.

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

EMC Response: Virtustream has built redundancy into all layers of the physical infrastructure in order to deliver SLAs up to 99.999% and mitigate any known risks. To further mitigate against the unknown, Core µVM's are designed for mission-critical workloads and include reserved compute capacity in a secondary datacenter and automatic storage replication to facilitate the ability to restore operations in the event of an outage at the primary data center.

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.

EMC Response: Virtustream's U.S. based data centers are located in Washington, DC, Las Vegas, and San Francisco. All data centers meet the highest industry standard in terms of operational protocol and have redundancy built into all layers of the physical infrastructure. Core µVM's, which are used for mission-critical workloads, provide reserved compute capacity and automatic storage replication so that these systems can be failed over to a secondary data center and have access to the compute capacity required in the event of a catastrophic outage at the primary data center.

Solution Administration

8.16 (E) SOLUTION ADMINISTRATION

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

EMC Response: Virtustream can provide managed solutions for Active Directory or LDAP. As a standard, we provide support for managing the VM itself and all OS support. However, our typical use case is where a customer manages the users and related activities, as Virtustream might not be aware of internal HR elements of User Management.

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

EMC Response: Virtustream offers Anti-Virus protection based on per virtual machine, per month charge.

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

EMC Response: The following serves as a checklist for removal of an existing customer environment from the Virtustream xStream Cloud.

Process Initiation

The Offboarding process shall be initiated only by a designated Senior Virtustream executive by creating a Service Request ticket in the xOC ticketing system and alerting the Accounting group to cease invoicing.

Process Checklist

Upon process initiation, the removal of services will be accomplished through xOC Change tickets to the respective Virtustream Departments following the Normal Approval process. The process will be scheduled following a Change Advisory Board (CAB) review and accomplished in the following order:

Table 21.   Offboarding Process Checklist

ORDER	SERVICES	GROUP RESPONSIBLE	DESCRIPTION
1	Security Services	SecOps	Removal of any Security related services such as Antivirus, Encryption, IDS, etc (if applicable)
2	CCS Services (SAP)	CCS	Removal of all SAP Basis resource permissions from Customer systems. Removal of all xOC alert groups for SAP resources (if applicable)
3	CCS Services (OS/Monitoring)	CCS	Removal of all Nimsoft probes and Hubs from the customer environment. (if applicable)
4	Backup services	CPS Backup Team	If requested from the customer, a final Full backup will be taken of the Customer systems and retained based on pre-existing expiration periods. Removal of Asigra DS-Clients will be scheduled for after the Expiration period of backups within the system
5	CPS	CPS/Onboarding	Removal of all customer VMs from the tenant environment
6	Network services	NetOps	Removal of all VRF/Firewall contexts, IPSec configurations, and IP subnets
7	Storage	CPS Storage Team	Removal of all Customer Aggregates, LUNS, and Datastores assigned to the Customer
8	IaaS	CPS Ops	Removal of remaining customer Resource Pools assigned to the customer
9	Portal	Portal Support	Removal of customer tenant and user accounts within the xStream Portal
10	xOC	xOC	Removal of customer Authorizations within the xOC helpdesk system.

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

EMC Response: Virtustream's Enterprise Cloud is based on a multi-tenancy cloud operating principle. We provide shared and in some cases dedicated infrastructure to support specific customer use cases. In the latter sense if there are custom processes and procedures that need to be supported within that dedicated environment Virtustream can look to qualify those use case scenarios to meet the requesting customers' needs. The majority of the management tool stacks and the processes and procedures are consistent across the environment to support standards and quality of service.

8.16.5 Ability to apply a participating entity's defined administration polices in managing a solution.

EMC Response: Virtustream's Enterprise Cloud is based on a multi-tenancy cloud operating principles. Similar to 8.16.4, any application of process and procedures for another Participating Entities' administration policies within the environment would need to be in a dedicated environment and not within the Virtustream Enterprise Cloud multi-tenant environment.

Hosting and Provisioning

8.17 (E) HOSTING AND PROVISIONING

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

EMC Response: Virtustream provides documentation for all of its software solutions. Attached to the RFP is the "xStream Portal User Guide" which outlines the process. xStream supports a vSphere virtualization stack from 5.1 to current 6.x releases. In addition, OpenStack KVM is supported. Any solutions that support either of those products will be useable with xStream.

8.17.2 Provide tool sets at minimum for:

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

EMC Response: Virtustream offers on-demand self-service portal where Participating Entities can deploy new servers as stand-alone or part of a server farm.

2. Creating and storing server images for future multiple deployments

EMC Response: Virtustream offers server images, templates, or other methods (OVF and blueprints) for multiple deployments as part of standard solution.

3. Securing additional storage space

EMC Response: Virtustream allows any VM Instance to be modified, including adding additional disks, memory and CPU's.

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).

EMC Response: Monitoring tools for use by each jurisdiction's authorized personnel are as follows:

Unified Dashboards

To monitor the health of NASPO's landscape, including but not limited to availability, a number of tools would be used. These tools track alarms at the hardware and application level, analyze trends, and provide views into server and application health. These readings are combined into unified dashboards, which are visible to clients, basis team members, DBA's, and OS and platform support teams.

Role of the xOC

This information is collated and funneled to a centralized command center, which we refer to as Virtustream's xStream Operations Center (xOC). The xOC coordinates all support activities, providing a single point of contact for all infrastructure and operations support. The xOC acts as a command center, with the below responsibilities:

- **Operations Center**: Ensuring production services are delivered effectively 24x7.
- **Service Request**: Responding to requests from customers.
- **Event Management**: Monitoring and management of events impacting Production services.
- **Incident Management**: Resolving incidents which impact services and restoring those services to production readiness as quickly as possible including RCA's.

- **Problem Management:** Prevent Incidents from happening and minimize impact from Incidents which can't be prevented.
- **Change Management**: Coordinate scheduled Changes within the Production environment.

Specifics on Alert Points

Alerts are proactive measures. Where possible, the alerting thresholds are set so that the Virtustream engineers can resolve issues before a fault occurs. Where this is not possible, the alerts at a minimum inform the support staff that a fault has occurred that needs resolution.

On those occasions when a fault occurs, a ticket will be raised automatically in the Nimsoft ticketing system used by Virtustream. Any Updates made to tickets by either party are visible via the Web Interface to the system. During an incident, a conference bridge is held open and periodic updates are sent by the xOC.

Below are the default monitoring metrics for the operating system and database. Thresholds can be tuned and additional objects added to meet client specific requirements:

Operating System Monitor Default Objects

Table 22. Operating System Monitor Default Objects

METRIC NAME	ALERT CRITICAL	ALERT – MAJOR	SAMPLES X FREQUENCY
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

Database Monitor Default Objects

Table 23. Database Monitor Default Objects

MONITOR	NOTES	DEFAULT THRESHOLD/VALUE	ALERT
Database Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical

MONITOR	NOTES	DEFAULT THRESHOLD/VALUE	ALERT
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with database performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any database resources.	This number should be "0" or "0" % wait time.	critical

The service level monitoring includes:

Table 24.   Service Level Monitoring

SERVICE CODE	SERVICE NAME	SERVICE DESCRIPTION	FREQUENCY
SVM001	System Availability	Checks that the IaaS is available and accessible.	<1 minute
SVM002	Version Management	Details the current version levels in operation.	On Request
SVM003	Background Jobs	Check for failed background jobs. Based on Customer guidelines.	Automate via CCMS alerting
SVM005	IDOC Status	Check the status of the in-coming and out-going IDOC queues. Based on Customer guidelines	Queues will monitored continuously and can be reset if in a stuck status, errors or issues will need to be addressed by the clients middleware technical or functional team member
SVM006	RFC Communications	Check the status of the inbound and outbound communication queues. Based on Customer guidelines	Multiple times per day depending on which queue
SVM008	Response Times	Check the dialog response time.	Daily or upon request or as part of issue RCA

SERVICE CODE	SERVICE NAME	SERVICE DESCRIPTION	FREQUENCY
SVM009	Memory Management	Check buffers.	Daily
SVM010	CPU Efficiency	Check CPU utilization.	<1 minute
SVM011	System Security	Check that system has been locked against system modification and that as determined by the Customers predefined strategy is enforced.	<1 minute
SVM013	Update Failures	Check for failed updates.	Daily
SVM014	Lock Management	Check for long running lock enqueues.	<1 minute
SVM015	SAP Processes	Check for long running processes.	<1 minute
SVM016	Active Users	Monitor user activity in support of annual SAP license auditing.	On Request
SVM018	Backup	Checks that backups have been successfully completed. Check the timing/performance of backups.	Daily
SVM019	Output Management	Check for spool failures.	Daily or per ticket request
SVM020	System Log	Check for critical or high warnings.	Daily
SVM022	File System Space	Check file system free space.	<1 minute

At the SAP level, in addition to all the automated tools, Virtustream has an "eyes on glass" monitoring team crawling the SAP systems throughout the day. This team covers a customized checklist at least three times per day, as shown below:

- Blended support model utilizing on shore & off shore
- Priority issues covered with blended model
- First responder performs initial triage and escalates as required
- Ticket acknowledgement within 30 minutes
- Customized check lists executed 3 times per day
- Lists are based on clients requirements and applications deployed
- Reports executed by offshore monitoring team
- Reports distributed to support staff and reviewed by support staff

Sample Eyes on Glass Report

Figure 20.   Sample Eyes on Glass Report

7:00 AM	11:00 AM	5:00 PM

Should NASPO choose to proceed further with Virtustream, the specific alerting points, and the tickets that would be triggered from them, would be documents in a monitoring and alert management standard operating procedure (SOP).

Trial and Testing Periods (Pre- and Post- Purchase)

8.18 (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE)

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

EMC Response: Trial and Test periods are offered for fee and can be set up to meet production requirements. Customer may request a proof-of-concept (PoC) to set up a sample workload in the Virtustream cloud for a limited period of time, generally 1-2 months to set-up, migrate data (if any), and test the PoC system. Prior to giving approval, Virtustream will work with the customer to define the success criteria of the PoC as well as next steps.

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

EMC Response: Virtustream will work with the customer to provision the PoC environment that will be consistent with the customer's production requirements. Details regarding length, cost, and success criteria will be discuss at the time the PoC is required.

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

EMC Response: PoC engagements receive the same level of support as regular customers in that the Service Desk will provide support and diagnostics services, training on how to use the xStream portal etc.

Integration and Customization

8.19 (E) INTEGRATION AND CUSTOMIZATION

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

EMC Response: Virtustream's xStream solution supports vSphere integration out of the box, using vCenter a central point of that integration. Additionally we support the REST API and anything that can be done via the User Interface can be done programmatically via REST API calls. Moreover, xStream also is capable of sending specific email formats into other systems such as ServiceNow or Remedy to support email integration capabilities.

Finally, xStream includes AppDirector. AppDirector has the capability to create System Controllers. System Controllers are used to provide a proxied Command Line Interface (CLI) to a group of systems which have been identified as Managed Systems for the specific System Controller. Using the Scheduler function within xStream, the end user is then able to run a specific task, script, or other available process from the System Controller against a single VM instance or a number of VM instances. These tasks or scripts can be setup to do anything from deploying an SAP install, formatting disks, applying patch sets, or updating accounts. The capability is only limited by the scripts available.

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

EMC Response: Virtustream's xStream solution allows for customizing the images, menu options, links, email addresses, content of auto-generated emails, and the user guide available in the xStream Portal. You can display up to 3 Links in the header, show 4 different branded images, and specify the email addresses used for the emails sent by the system during provisioning and other related tasks. All of these tasks are described in detail in the "CSP Customization Guide" which is available upon request.

Marketing Plan

8.20 (E) MARKETING PLAN

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

EMC Response: EMC will market the NASPO ValuePoint contract directly to buyers and VARs with a full rollout of these activities:

- Online Promotion
  - EMC NASPO ValuePoint website
  - Product-specific educational webinars
  - Regular tweets from @EMCPublicSector twitter handle
  - Social amplification through EMC SLED Alliances team
- Collateral
  - Printed data sheet
  - Electronic brochure (PDF downloadable version on website)
  - Signs for use at trade shows

- Trade Shows and Industry Events
  - EMC participates in nearly 50 regional and national industry events each year. Events include CA CIO Academy, NYC Tech Forum, CCISDA, MISAC Massachusetts Digital Government summit and more. For the life of the contract, EMC will appropriately represent the EMC NASPO ValuePoint contract at the events.
  - Over a dozen speaking engagements per calendar year will be scheduled.
  - Major sponsorships at NASCIO, NASTD, and NACo will be provided.
  - C-level sponsorships include Digital States Performance Institute (DSPI), GOVERNING Women in Government Leadership Program, RSA Conference Public Sector.
- Advertising
  - Print: Conference-specific hard-copy handouts
  - Online: TechWire, Government Technology/Navigator website, GovTech Justice and Public Safety Web Channel, partner.emc.com
  - Thought Leadership Supplements with Government Technology and Public CIO

EMC will also provide marketing kits to its EMC NASPO ValuePoint authorized VARs to help them promote the NASPO ValuePoint Participating Addenda (PAs). The kits will includes sample tweets, a link to the PA for that State, and a sample press release for the VAR to customize and publish.

We will execute these NASPO ValuePoint marketing activities throughout the life of the contract in an effort to keep awareness high.

Related Value-Added Services to Cloud Solutions

8.21 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS

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

EMC Response: Virtustream offers xStream, a secure, high performance cloud platform, which provides high availability, highly secure enterprise class clouds, with application level monitoring and SLAs.

The xStream solution is available both as a software solution for use with existing enterprise data centers/clouds, as an appliance for stand-alone use and also as a managed service delivered from Virtustream's virtual private cloud.

Customers can select the optimal solution - on–premise, off-premise, hybrid, software based or managed services to fit their cloud evolution and deployment requirements.

To further enhance their solutions and to help enterprises begin to move to the cloud Virtustream offers assistance with planning, migrating and operating applications to the cloud.

EMC's Virtustream offer provides Participating Entities with a full portfolio of cloud professional services to support their migration to the cloud:

- IT Transformation Workshop will accelerate the ability to deliver IT as a service and become a broker of private and public cloud services to the business. It helps identify gaps in customer's current state and provides recommended steps for cloud transformation. A pre-workshop questionnaire gathers the perspective of the customer's business and IT stakeholders on key IT goals and challenges. Based on answers to the questionnaire, EMC will prepare a gap analysis, benchmarking the customer organization's transformation readiness against their industry peers. Also, based on the gaps identified, EMC develops a set of recommendations tailored to the customer's situation, including a projected return on investment (ROI) analysis. Then, during a half-day on-site session, our team of transformation experts works with the customer's key IT executives to:

  - Review the results of the gap analysis and benchmark data
  - Discuss the recommendations and review the financial impact of executing them
  - Prioritize next steps and gain consensus among your executive team

  After the workshop, EMC will provide you with a transformation report that includes an executive-level summary documenting the workshop results as well as the benchmarks showing how your organization compares to the best peers in your industry across your application, infrastructure and operating models, along with recommendations for next steps you can take to achieve your transformation objectives.

- Cloud Advisory Services helps achieve the right mix of private, public, and hybrid cloud delivery models for key customer application workloads. EMC provides a cloud application strategy that is specific to the needs and activities of the customer, recognizes the customer's current IT capabilities, and understands how service provider partners can provide complementary services to the customer's own IT infrastructure.

  EMC also helps execute the customer's strategy using an innovative, tool-based approach to workload analysis that places workloads in the optimal private, public, or hybrid cloud model by analyzing customer business and technology requirements. Service deliverables include:

  - Business Application Alignment—maps selected applications to associated business processes to validate relevance and service levels for the business activity, using the EMC Planning Studio toolset to assure a consistent evaluation across your business

  - Application Suitability Assessment for Cloud—examines your business requirements for selected application workloads and determines whether they are best delivered through a private cloud, public cloud, or legacy IT environment, using the EMC Planning Studio toolset

  - Workload Placement Analysis—EMC consistently analyzes these selected application workloads to determine their optimal cloud delivery model, including recommendations for specific public cloud services providers, based on customer specific business and technology architectural considerations, using the EMC Design Studio toolset

- Cloud Cover Services offer the full range of monitoring and management services for core cloud/DC infrastructure through to enterprise applications and database support.

- Cloud Staging and Networks provide colocation, security and network services to assist customers as they migrate to the cloud.

Here is a list of services, and a full and comprehensive solution can be provided as required by Participating Entities:

Table 25.   IaaS Onboarding and Migration

PRODUCT NAME	DESCRIPTION
IaaS Onboarding - Virtustream Led	Virtustream will provision platform resources and migrate Customer systems to the Virtustream cloud.
IaaS Onboarding - Self-Service	Virtustream will enable a secure connection to the Virtustream cloud and provision IaaS resources. After Virtustream-led training, Customer will migrate their systems to the Virtustream cloud.
IaaS Onboarding - Project Based	Virtustream will enable a secure connection to the Virtustream cloud and provision IaaS resources. All other responsibilities as agreed between Virtustream and Customer, per Customer requirements.
IaaS Migration Support (IaaS Onboarding Charge) - Project Based	Virtustream will assess Customer requirements, define a migration plan, and execute system migration, per plan.

Table 26.   IaaS Compute

PRODUCT NAME	DESCRIPTION
Enterprise Basic Plus µVM	Enterprise Basic Plus µVMs are used for non-production or production, non-Internet-accessible workloads.
Reserved µVM	. A customer ordered quantity of non-operating µVMs are reserved at a secondary Virtustream data center for ongoing operation during disaster events and during scheduled disaster recovery (DR) exercises.
High Memory Enterprise Basic Plus VM Fee	Surcharge Must be paired with *High Memory Enterprise Basic µVM Fee* (directly below).
High Memory Enterprise Basic Plus µVM	High Memory Enterprise Basic Plus µVMs are recommended for >64 GB VM. Must be paired with *High Memory Enterprise Basic Plus VM Fee* (directly above). Enterprise Basic Plus µVMs are used for non-Internet-accessible workloads.

Table 27.   IaaS HANA Physical Appliances

PRODUCT NAME	DESCRIPTION
HANA Appliance Installation and Setup - Physical Appliance	Setup and configuration of a Physical HANA managed appliance.
HANA Migration and Optimization	Migration and optimization of Customer's database into the HANA managed appliance.
6 TB HANA Managed Appliance for SOH - Primary	Dedicated 6TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)

PRODUCT NAME	DESCRIPTION
6 TB HANA Managed Appliance for SOH - Secondary	Dedicated 6TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
3 TB HANA Managed Appliance for SOH - Primary	Dedicated 3TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
3 TB HANA Managed Appliance for SOH - Secondary	Dedicated 3TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
2 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
2 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's - Secondary Virtustream data center. (Hardware only.).
2 TB HANA Managed Appliance for BW (Scale-Out) - Primary	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
2 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
2 TB HANA Managed Appliance for SOH - Primary	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
2 TB HANA Managed Appliance for SOH - Secondary	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
1.5 TB HANA Managed Appliance for SOH - Primary	Dedicated 1.5TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
1.5 TB HANA Managed Appliance for SOH - Secondary	Dedicated 1.5TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).

PRODUCT NAME	DESCRIPTION
1 TB HANA Managed Appliance (Single-Node/Scale-Up) - Primary	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
1 TB HANA Managed Appliance (Single-Node/Scale-Up) - Secondary	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
1 TB HANA Managed Appliance for BW (Scale-Out) - Primary	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
1 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
1 TB HANA Managed Appliance for SOH - Primary	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
1 TB HANA Managed Appliance for SOH - Secondary	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
512 GB HANA Managed Appliance (Single-Node/Scale-Up) - Primary	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
512 GB HANA Managed Appliance (Single-Node/Scale-Up) - Secondary	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
512 GB HANA Managed Appliance for BW (Scale-Out) - Primary	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
512 GB HANA Managed Appliance for BW (Scale-Out) - Secondary	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).

PRODUCT NAME	DESCRIPTION
256 GB HANA Managed Appliance (Single-Node/Scale-Up) - Primary	Dedicated 256GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
256 GB HANA Managed Appliance (Single-Node/Scale-Up) - Secondary	Dedicated 256GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
128 GB HANA Managed Appliance (Single-Node/Scale-Up) - Primary	Dedicated 128GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
128 GB HANA Managed Appliance (Single-Node/Scale-Up) - Secondary	Dedicated 128GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)

Table 28.   OS, Database, and Other Software

PRODUCT NAME	DESCRIPTION
Microsoft SQL Standard (Per 2 cores)	Microsoft SQL Server, Standard Edition license for unlimited users per month.
Microsoft SQL Enterprise (Per 2 cores)	Microsoft SQL Server, Enterprise Edition license for unlimited users per month.
SUSE Linux Enterprise ≤ 2 vCPU & ≤ 2GB RAM	SUSE Linux Enterprise Server for x86&x86-64, per hosted instance.
SUSE Linux Enterprise ≤ 4 vCPU & ≤ 8GB RAM	SUSE Linux Enterprise Server for x86&x86-64, hosted instance.
SUSE Linux Enterprise ≤ 8 vCPU & > 8GB RAM	SUSE Linux Enterprise Server for x86&x86-64, hosted instance.
SUSE Linux Enterprise > 8 vCPU or > 8GB RAM	SUSE Linux Enterprise Server for x86&x86-64.

PRODUCT NAME	DESCRIPTION
SUSE Linux Enterprise for SAP ≤ 2 vCPU & ≤ 2GB RAM	SUSE Linux Enterprise Server for x86&x86-64, hosted instance. Optimized for use with SAP.
SUSE Linux Enterprise for SAP ≤ 4 vCPU & ≤ 8GB RAM	SUSE Linux Enterprise Server for x86&x86-64, hosted instance. Optimized for use with SAP.
SUSE Linux Enterprise for SAP > 4 vCPU or > 8GB RAM	SUSE Linux Enterprise Server for x86&x86-64, hosted instance. Optimized for use with SAP.
SUSE Linux Enterprise for Physical HANA	SUSE Linux Enterprise Server for x86&x86-64. For use on physical HANA appliances.
Red Hat Enterprise Linux - Standard (Per OS)	Red Hat Enterprise Linux, Standard, for four or fewer vCPUs.
Red Hat Enterprise Linux – Enterprise (Per OS)	Red Hat Enterprise Linux, Enterprise, for five or more vCPUs.
Microsoft OS	Windows Server OS.

Table 29. IaaS Storage & Backup

PRODUCT NAME	DESCRIPTION
System Backup Setup	Setup and configuration of Customer's backup environment.
System Backup - Replicated	File system backup at Customer's primary Virtustream data center on a periodic basis. Backups are replicated to Customer's secondary Virtustream data center.
System Backup - Local Only	File system backup at Customer's primary Virtustream data center on a periodic basis.
Tier 0 Block Storage – Local Only	Tier 0 local block Storage with 3ms Latency Service Level, maintained in a single data center.
Tier I Block Storage – Local Only	Tier I local block Storage with 10ms Latency Service Level, maintained in a single data center.
Tier II Block Storage – Local Only	Tier II local block Storage with 20ms Latency Service Level, maintained in a single data center.
Tier III Block Storage – Local Only	Tier III local block Storage w/ 40ms Latency Service Objective, maintained in a single data center.

PRODUCT NAME	DESCRIPTION
Tier 0 Block Storage – Replicated	Tier 0 replicated block Storage w/ 3ms Latency Service Level persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.
Tier I Block Storage – Replicated	Tier I replicated block Storage w/ 10ms Latency Service Level persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.
Tier II Block Storage – Replicated	Tier II replicated block Storage w/ 20ms Latency Service Level persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.
Tier III Block Storage – Replicated	Tier III replicated block Storage w/ 40ms Latency Service Objective persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Table 30. IaaS Network

PRODUCT NAME	DESCRIPTION
Network Bandwidth Fee - USDC1	Internet-facing bandwidth to/from Virtustream's Washington, DC data center.
Network Bandwidth Fee - USDC2	Internet-facing bandwidth to/from Virtustream's San Francisco, CA data center.
Network Bandwidth Fee - USDC3	Internet-facing bandwidth to/from Virtustream's Las Vegas, NV data center.
Network Bandwidth Fee - UKDC1	Internet-facing bandwidth to/from Virtustream's UK data center.
Network Bandwidth Fee – NLDC1	Internet-facing bandwidth to/from Virtustream's NL data center.
Public IP Address (IPv6)	Per assigned public IPv6 IP address block per month.
Public IP Address (IPv4)	Per assigned public IPv4 IP address per month.

Table 31.   IaaS Load Balancer

PRODUCT NAME	DESCRIPTION
Load Balancer Setup – Basic	Template provided to Customer for service list and rule preferences; Virtustream configures.
Load Balancer Setup - Advanced	Technical briefing with Customer to determine sizing and level of effort.
Load Balancing Fee (Additional to Network Bandwidth)	Fee for load balancer bandwidth use.
Managed Load Balancer Services (Per Server)	Virtustream-managed load balancer facilitates Customer load balancer configuration change requests.

Table 32.   IaaS Cloud & Storage Connect

PRODUCT NAME	DESCRIPTION
Cloud Connect - Standard (24 ports available) - Setup - USDC1	Installation of one 24-port, gigabit network switch in Virtustream's Washington, DC data center.
Cloud Connect - Standard (24 ports available) - USDC1	One 24-port gigabit network switch providing colocation-to-cloud connectivity in Virtustream's Washington, DC data center.
Cloud Connect - HA (48 ports available) - Setup - USDC1	Installation of two 24-port, gigabit network switches (for High Availability) in Virtustream's Washington, DC data center.
Cloud Connect - HA (48 ports available) - USDC1	Two managed, 24-port gigabit network switches (for a total of 48 ports) providing High Availability (HA) colocation-to-cloud connectivity in Virtustream's Washington, DC data center.
Cloud Connect - Standard (24 ports available) - Setup - USDC2	Installation of one 24-port, gigabit network switch in Virtustream's San Francisco, CA data center.
Cloud Connect - Standard (24 ports available) - USDC2	One 24-port gigabit network switch providing colocation-to-cloud connectivity Virtustream's San Francisco, CA data center.
Cloud Connect - HA (48 ports available) - Setup - USDC2	Installation of two 24-port, gigabit network switches (for High Availability) Virtustream's San Francisco, CA data center.

PRODUCT NAME	DESCRIPTION
Cloud Connect - HA (48 ports available) - USDC2	Two managed, 24-port gigabit network switches (for a total of 48 ports) providing High Availability (HA) colocation-to-cloud connectivity Virtustream's San Francisco, CA data center.
Cloud Connect - Standard (24 ports available) - Setup - UKDC1	Installation of one 24-port, gigabit network switch in Virtustream's London data center.
Storage Connect - Standard - Setup - USDC1	Installation of one Fiber Channel switch in Virtustream's Washington, DC data center.
Storage Connect - Standard - USDC1	Single Fiber Channel switch providing Storage connectivity in Virtustream's Washington, DC data center.
Storage Connect - HA - Setup - USDC1	Installation of two Fiber Channel switches in Virtustream's Washington, DC data center.
Storage Connect - HA - USDC1	Dual Fiber Channel switches providing Storage connectivity in Virtustream's Washington, DC data center.
Storage Connect - Standard - Setup - USDC2	Installation of one Fiber Channel switch in Virtustream's San Francisco, VA data center.
Storage Connect - Standard - USDC2	Single Fiber Channel switch providing Storage connectivity San Francisco, VA data center.
Storage Connect - HA - Setup - USDC2	Installation of two Fiber Channel switches San Francisco, VA data center.
Storage Connect - HA - USDC2	Dual Fiber Channel switches providing Storage connectivity San Francisco, VA data center.

Table 33.   IaaS Ad Hoc Services

PRODUCT ID	PRODUCT NAME	BILLING	DESCRIPTION
IC-SVC-DR-PROJ	DR Test Planning	Project based	Disaster Recovery (DR) Test Planning process produces Customer-specific DR Test Plan that specifies the scope of VMs, VLANs, and Storage (Data Stores) to be tested, is specific to the customer environment, and can be conducted with minimal disruption to the customer's on-going production workload.

PRODUCT ID	PRODUCT NAME	BILLING	DESCRIPTION
IC-SVC-DR1-AH	DR Test Service Tier 1 (10 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 10 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR2-AH	DR Test Service Tier 2 (20 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 20 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR3-AH	DR Test Service Tier 3 (40 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 40 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR4-AH	DR Test Service Tier 4 (80 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 80 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR5-AH	DR Test Service Tier 5 (160 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 160VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR6-AH	DR Test Service Tier 6 (320 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 320 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-RPT-VRS-REQ	Virtualization Right Sizing Report	one time, per report	Right Sizing report showing configured versus actual usage with recommendations on CPU and memory for up to 500 VMs.
IC-RPT-VCC-REQ	Virtualization Custom Consumption Report	one time, per report	Custom consumption report for up to 500 VMs showing compute and storage utilization broken down by VM and resource pool.
IC-DP-BU-CRS	Backup Restoration Request with CCS	one time, per restoration	Additional Backup Restorations beyond the included 10-per-month; for Customers with Virtustream Cloud Cover Services.
IC-DP-BU-NRS	Backup Restoration Request without CCS	one time, per restoration	Additional Backup Restorations beyond the included 10-per-month; for customers without Virtustream Cloud Cover Services.

Security Services - Network Based (Perimeter Defense): Overview

Table 34.   Firewall

PRODUCT ID	PRODUCT NAME	BILLING	DESCRIPTION
CS-FW-FW-1T	Firewall Configuration/Setup	one time, per firewall	Firewall configuration and setup fee; required for each location with Internet-facing bandwidth.
CS-FW-MPF-SVC	Managed Perimeter Firewall	monthly, per VM	Virtustream-managed firewall service facilitates Customer firewall configuration change requests.

Table 35.   IPSec VPN

PRODUCT NAME	DESCRIPTION
IPSec VPN Host-Side Configuration	IPSec VPN Tunnel configuration/management at the Virtustream data center.
IPSec VPN Client-Side Configuration	Remote support of Customer's configuration of the IPSec VPN Tunnel at Customer site.
IPSec VPN Bandwidth Fee - USDC1	IPSec VPN Bandwidth between Customer site and Virtustream's Washington, DC Data Center.
IPSec VPN Bandwidth Fee - USDC2	IPSec VPN Bandwidth between Customer site and Virtustream's San Francisco, CA Data Center.
VPN Tunnel Managed Service Fee	Maintenance of circuit between Virtustream data center and Customer's facility.

Table 36.   Intrusion Detection Service (IDS) - Network-based

PRODUCT NAME	DESCRIPTION
Network Based Intrusion Detection Primary Site Setup	Intrusion Detection Services (IDS) installation and configuration at Customer's primary Virtustream data center.
Network Based Intrusion Detection System and Managed Service Fee - Primary	Managed service for the network-based Intrusion Detection Service (IDS) at Customer's primary Virtustream data center.
Network Based Intrusion Detection Second Site Setup	Intrusion Detection Services (IDS) installation and configuration at Customer's secondary Virtustream data center.
Network Based Intrusion Detection System & Managed Service Fee - Secondary	Managed service for the network-based Intrusion Detection Service (IDS) at Customer's secondary Virtustream data center.

Security Services - VM-Level: Overview

Table 37.   Anti-Virus / Anti-Malware (AV/AM) - VM-based

PRODUCT NAME	DESCRIPTION
Anti-Virus Primary System Setup	Virtustream will deploy an anti-virus / anti-malware system to Customer specifications in Customer's primary Virtustream data center.
Anti-Virus Primary System	Includes threat updates, patches, minor service pack releases, and major system upgrades for the AV / AM system at Customer's primary Virtustream data center.
Anti-Virus Secondary System Setup	Virtustream will deploy an anti-virus / anti-malware system to Customer specifications in Customer's secondary Virtustream data center.
Anti-Virus Secondary System	Includes threat updates, patches, minor service pack releases, and major system upgrades for the AV / AM system at Customer's secondary Virtustream data center.

Table 38.   Intrusion Detection Service (IDS) - VM-based

PRODUCT NAME	DESCRIPTION
Intrusion Detection and Firewall Primary System Setup	Setup of VM-level IDS and firewall in Customer's primary Virtustream data center.
Intrusion Detection and Firewall Primary System	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the IDS system at Customer's primary Virtustream data center.
Intrusion Detection and Firewall Secondary System Setup	Setup of VM-level IDS and firewall in Customer's secondary Virtustream data center.
Intrusion Detection and Firewall Secondary System	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the IDS system at Customer's secondary Virtustream data center.
Intrusion Detection and Firewall Managed Service	Virtustream manages all IDS and firewall rule change requests.

Table 39.   File Integrity Monitoring (FIM)

PRODUCT NAME	DESCRIPTION
File Integrity Monitoring Primary System Setup	Virtustream will install and configure a single instance of File Integrity Manager (FIM) at Customer's primary Virtustream data center based on Customer specifications.
File Integrity Monitoring Primary System	Includes patches, minor service pack releases, and major system upgrades for the FIM system at Customer's primary Virtustream data center.
File Integrity Monitoring Secondary System Setup	Virtustream will install and configure a single instance of File Integrity Manager (FIM) at Customer's secondary Virtustream data center based on Customer specifications.
File Integrity Monitoring Secondary System	Includes patches, minor service pack releases, and major system upgrades for the FIM system at Customer's secondary Virtustream data center.
File Integrity Monitoring Managed Service	Virtustream will monitor Customer's VMs and notify Customer of alerts generated by the FIM.

Table 40.   VM-Level Security Bundle (VLSB)

PRODUCT NAME	DESCRIPTION
VM-Level Security Bundle Primary System Setup	Virtustream will consult with Customer, then deploy a Customer specific environment and with a Customer-specific policy configuration in Customer's primary Virtustream data center.
VM-Level Security Bundle Primary System fee	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the VLSB system at Customer's primary Virtustream data center.
VM-Level Security Bundle Secondary System Setup	Virtustream will consult with Customer, then deploy a Customer specific environment and with a Customer-specific policy configuration in Customer's secondary Virtustream data center.
VM-Level Security Bundle Secondary System fee	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the VLSB system at Customer's secondary Virtustream data center.
VM-Level Security Bundle Service Fee (<101 VMs)	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.
VM-Level Security Bundle Service Fee (<1,001 VMs)	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.
VM-Level Security Bundle Service Fee (<10,001 VMs)	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.

PRODUCT NAME	DESCRIPTION
VM-Level Security Bundle Service Fee (>10,000 VMs)	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.

Table 41. Encryption

PRODUCT NAME	DESCRIPTION
Encryption Management System Setup - SaaS	Configuration of Customer in shared encryption system to manage encryption agents.
Encryption Management System Setup - Dedicated	Setup and configuration of a Customer-specific, dedicated encryption system to manage encryption agents.
Encryption Management System Fee	Virtustream will monitor the operation of the encryption service and monitor for exceptions.
Encryption Agent Setup	Setup encryption agent for each VM. Agents enforce the encryption policy as defined in the encryption management system.
Encryption Production Agent per vCPU Fee	Fee covers agents in Customer's production environment.
Encryption Non-Production Agent per vCPU Fee	Fee covers agents in Customer's non-production environment.
High Memory Encryption Agent Setup	Setup encryption agent for each High Memory VM. Agents enforce the encryption policy as defined in the encryption management system.
High Memory Encryption Agent Fee (Production)	Fee covers agents on High Memory μVMs in Customer's production environment.
High Memory Encryption Agent Fee (Non-Production)	Fee covers agents on High Memory μVMs in Customer's non-production environment.

Table 42.   Vulnerability Scanning

PRODUCT NAME	DESCRIPTION
Vulnerability Scanning Managed Service - non Public IP	Scanning of non-public IP endpoints within the customer's Virtustream environment; generates reports on possible network vulnerabilities. Virtustream security personnel will provide monthly feedback and suggested prioritization of issues.
Vulnerability Scanning Managed Service - Public IP	Scanning of public IP endpoints within the customer's Virtustream environment; generates reports on possible network vulnerabilities. Virtustream security personnel will provide monthly feedback and suggested prioritization of issues.

Table 43.   Log Management

PRODUCT NAME	DESCRIPTION
Log Management System Setup	Configuration of the Log Management System to support log management requirements.
Managed Log Management Service Setup	Installation and configuration of the log management system.
Log Management System Fee	Fee for monthly management of the log aggregation system.
Managed Log Management Service	Service fee for monthly management and monitoring of log aggregation system use, including log capacity recommendations.

Table 44.   Security Policy Audit Services

PRODUCT NAME	DESCRIPTION
Firewall Audit System Setup	Virtustream installation and configuration of the Firewall Audit Management System.
Firewall Audit Export Setup	Configuration and testing of Customer designated firewall in the Virtustream cloud to export settings to the Firewall Audit Manager.
Firewall Audit System	Virtustream maintenance of the Firewall Audit system, which monitors changes to the network security policy and provides a complete audit trail.
Managed Firewall Auditing Service	Virtustream will the export the data from managed firewalls on a monthly basis, and perform analysis of supported firewalls as a scheduled audit.
Policy Auditor System Setup	Service includes the tasks necessary to install a dedicated FWPA system within the Customer's environment
Policy Auditor Service Setup	Service includes the tasks required to configure a customer in either the Shared Firewall Policy Auditing System or a Dedicated Policy Auditor System.
Policy Auditor System Fee	This fee covers compute resources to support the Dedicated Policy Auditor deployment, including VM, OS, Memory, I/O, Storage, networking.
Policy Auditor Service Fee	Fee for the performance of the firewall policy analysis. Deliverables include: Risky Rule report, Rule Optimization Report, PCI Compliance Report.

Table 45.   Two-Factor Authentication (2FA)

PRODUCT NAME	DESCRIPTION
2FA Virtustream Portal Token Issue	Virtustream will register a 2FA token for the Virtustream Portal, and provide users with information and, when necessary, training for how to use tokens.
2FA Virtustream Portal Token Fee	Fee for ongoing use of each 2FA token for the Virtustream Portal.
2FA Dedicated Setup	Virtustream will install and configure a single instance of 2FA management system on a per Tenant basis.
2FA Dedicated Self-Service Setup	Customer will install and configure a single instance of the 2FA Management System on a per Tenant basis.
2FA Dedicated Base Fee	Monthly fee for a single instance of a Customer's dedicated 2FA Management System at Customer's primary Virtustream data center.
2FA Dedicated DR Setup	Virtustream will install and configure a single instance of the 2FA Management System on a per Tenant basis in Customer's secondary Virtustream data center.
2FA Dedicated DR Base Fee	Monthly fee for a single instance of a Customer's dedicated 2FA Management System at Customer's secondary Virtustream data center.
2FA Dedicated Token Issue	Customer personnel will issue and install a 2FA token on a mobile device or computer.
2FA Dedicated Token Fee	Monthly fee for the use of 2FA Tokens associated with the 2FA Management System.
2FA Shared Setup	Virtustream will assist Customer in setting up an account in Virtustream's Shared 2FA Management System.
2FA Shared Self-Service Setup	Customer will set up an account in Virtustream's Shared 2FA Management System. Virtustream will supply Customer with information required to integrate to Customer's designated Active Directory (AD).
2FA Shared Token Issue	Customer personnel will issue and install a 2FA token on a mobile device or computer.
2FA Shared Token Fee	Monthly fee for the use of 2FA Tokens associated with the 2FA Management System.

Colocation Services: Overview

Table 46.   Colocation Services

PRODUCT NAME	DESCRIPTION
Fiber Cross Connect - Vienna - Installation	Fiber Cross Connect Installation - Washington, DC data center.
Copper Cross Connect - Vienna - Installation	Copper Cross Connect Installation - Washington, DC data center.

PRODUCT NAME	DESCRIPTION
Fiber Cross Connect - Vienna	Fiber Cross Connect - Washington, DC data center.
Copper Cross Connect - Vienna	Copper Cross Connect - Washington, DC data center.
Hotel Rack (1U) - Managed Colo - Vienna	2x 1G Copper interfaces per RU - Washington, DC data center; Remote Eyes & Hands required: DC-SVC-REU-B, -S, or -G.
Fiber Cross Connect - San Francisco - Installation	Fiber Cross Connect Installation - San Francisco, CA data center.
Copper Cross Connect - San Francisco - Installation	Copper Cross Connect Installation - San Francisco, CA data center.
Fiber Cross Connect - San Francisco	Fiber Cross Connect - San Francisco, CA data center.
Copper Cross Connect - San Francisco	Copper Cross Connect - San Francisco, CA data center.
Hotel Rack (1U) - Managed Colo - San Francisco	2x 1G Copper interfaces per RU; Remote Eyes & Hands required: DC-SVC-REU-B, -S, or -G
Remote Eyes & Hands (US) - Bronze	Bronze (9x5) 2 hours (Billed in 15 min increments).
Remote Eyes & Hands (US) - Silver	Silver (9x5) 5 hours (Billed in 15 min increments).
Remote Eyes & Hands (US) - Gold	Gold (24x7) 10 hours.
Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (15 Minutes)	15-minute increment of US Bronze or Silver service
Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (1 Hour)	1-hour increment of US Bronze or Silver service
Remote Eyes & Hands (US) - Gold Ad Hoc (15 Minutes)	15-minute increment of US Gold service

PRODUCT NAME	DESCRIPTION
Remote Eyes & Hands (US) - Gold Ad Hoc (1 Hour)	1-hour increment of US Gold service

Operating System is available as an Onshore service. One supported OS per VM.

Table 47.   Operating System Support

OPERATING SYSTEM SUPPORT			
CPT SKU	**PRODUCT NAME**	**DESCRIPTION**	**NOTES**
Onshore: CC-NS-ONOS-STD	**Standard** Operating System Support	• 24x7x365 monitoring of Customer's OS server environment and notification to Customer of threshold breaches. • Patching of Critical Microsoft only Operating System patches.	
Onshore: CC-NS-ONOS-BUS	**Business** Operating System Support	• 24x7x365 monitoring of Customer's OS server environment and notification to Customer of threshold breaches. • Monday – Friday 8:00 AM EST to 6:00 PM EST incident resolution and responses to Service Requests. • Capacity Management. • Operating System Management. • Patch Management.	Charged per VM and billed monthly.
Onshore: CC-NS-ONOS-ENT	**Enterprise** Operating System Support	• 24x7x365 monitoring of Customer's OS server environment and notification to Customer of threshold breaches. • 24x7x365 incident resolution. • Monday – Friday 8:00 AM EST to 6:00 PM EST responses to Service Requests. • Capacity Management. • Operating System Management. • Patch Management.	

Database Support

Operating System and Database Support is available as an Onshore service. Maximum two databases and one OS per VM.

Table 48.   Database & Operating System Support

DATABASE & OPERATING SYSTEM SUPPORT			
CPT SKU	**PRODUCT NAME**	**DESCRIPTION**	**NOTES**
Onshore: CC-NS-ONDB-STD	**Standard** Operating System and Database Support	• 24x7x365 monitoring of Customer's OS and RDBMS server environment and notification to Customer of threshold breaches. • Patching of Critical *Microsoft only* Operating System patches.	Charged per instance and billed monthly.
Onshore: CC-NS-ONDB-BUS	**Business** Operating System and Database Support	• 24x7x365 monitoring of Customer's OS and RDBMS server environment and notification to Customer of threshold breaches. • Monday – Friday 8:00 AM EST to 6:00 PM EST incident resolution and responses to service requests. • Capacity Management. • Database Management. • Operating System Management. • Patch Management for Operating Systems, Critical Patches for RDBMS.	
Onshore: CC-NS-ONDB-ENT	**Enterprise** Operating System and Database Support	• 24x7x365 monitoring of Customer's OS and RDBMS server environment and notification to Customer of threshold breaches. • 24x7x365 incident resolution, Monday – Friday 8:00 AM EST to 6:00 PM EST responses to Service Requests. • Capacity Management. • Database Management. • Operating System Management. • Patch Management for Operating Systems, Critical Patches for RDBMS.	

Technical Account Management Services (TAMS)

Table 49.   Technical Account Manager

TECHNICAL ACCOUNT MANAGER			
PRODUCT ID	**PRODUCT NAME**	**DESCRIPTION**	**NOTES**
CC-TAM-TAM-FULL	Technical Account Manager (TAM)	TAM is a customer account based service based on size and complexity of the Customer solution. TAM will coordinate day-to-day operation, service level management and SL reporting. This service is to be part of Virtustream offering (as further specified in a PO Agreement).	Available in quarter, half, full time, instance based, or as Ad Hoc sub services.
CC-TAM-TAM-HALF			
CC-TAM-TAM-QTR			
CC-TAM-TAM-INST			

Table 50.   Primary TAM Services Available to be Delivered

TAM SERVICES			
PRODUCT ID	**PRODUCT NAME**	**DESCRIPTION**	**NOTES**
CC-TAM-TAM-FULL	Technical Account Manager (TAM) - Full	TAM is a customer account based service based on size and complexity of the Customer solution. TAM will coordinate day-to-day operation, service level management and SL reporting. This service is to be part of Virtustream offering (as further specified in a PO Agreement).	"Strategic Partnership"
CC-TAM-TAM-HALF	Technical Account Manager (TAM) - Half		"Single Point of Contact for Mission Critical Activities & Quarterly Reviews"
CC-TAM-TAM-QTR	Technical Account Manager (TAM) - Quarter		"Operations Management"
CC-TAM-TAM-INST	Technical Account Manager (TAM) – Per Instance		

Table 51.   Responsibilities of and/or the Services to be Provided by the TAM.

DEFINITION	1/4 TAM	1/2 TAM	FULL TAM
Operations Management (Weekly and Monthly)			
SLA Management / Compliance / Reporting	X	X	X
Contract management	X	X	X
Proactive Statistical Analysis of Performance Data with recommendations to optimize performance and utilization (Rightsizing)	X	X	X
Best Practice recommendations and Run Optimization	X	X	X
Status Reporting (Weekly Checkpoint Meeting)	X	X	X
Respond to Customer question / handle Customer escalation requests	X	X	X
Incident Management & Central Coordination	X	X	X
Point of contact for requests for RCA	X	X	X
Facilitate Problem Management meeting with Customer to review RCA reports (as needed)	X	X	X
Track and report on Incident and Service Request ticket aging; facilitate prompt completion of any tickets aging beyond SLOs	X	X	X
Single Point of Contact for Mission Critical Activities & Quarterly Reviews			
Monitor the Services and proactively work with Customer to identify ongoing IT resource capacity *NOTE: Consumption will be part of the Monthly billing.*		X	X
Execute provisioning tasks from customer requests		X	X
Failover, D/R testing coordination		X	X
Operations Integration with Customer Processes (example: customer Change Management attendance)		X	X
Quarterly Business review		X	X
For contracted services, perform quarterly reviews of reliability and availability using: Service Level reporting; Service management statistics; Resource usage and trending; Project execution; Capacity management and trending; Root Cause Analyses; Event history in the ITSM System; Customer satisfaction data; Security Event history and trending; Disaster recovery plans		X	X
For Managed Services Platforms, perform a quarterly review of reliability and availability of the components of the Managed Services Platforms		X	X
Upon the completion of reviews, meet with Customer to propose improvements		X	X

DEFINITION	1/4 TAM	1/2 TAM	FULL TAM
Provide monthly reporting on service delivery (summary report of incident tickets & service requests including type, priority, min/mean/max time to complete, etc)		X	X
Provide copies of all run books to Customer and facilitate completion/updates for any run books and/or requested design documents		X	X
Strategic Partnership			
Access ongoing co-innovation and co-value realization			X
Strategic Roadmap and planning activities			X
Executive Scorecards			X
Brief Customer semi-annually on technology and process evolutions that may be of interest or beneficial to Customer			X
Assist Customer's BDPs and TDPs process such as providing: Specific, short-term steps and schedules for projects or changes expected to occur within the first twelve (12) months of each plan; Budgetary cost estimates to complete such projects; Reviews of Customer's business cases; Future volume projections, technology, and geographic changes that could impact Customer's systems and technical architectures			X
Facilitate quarterly demand management planning meetings			X
Conduct semi-annual Infrastructure architecture planning sessions with Customer to review Customer's current business objectives and related technology demands; discuss the current market view of relevant technologies, IT industry trends, and architecture approaches; document and update a three (3) year infrastructure roadmap and implementation plan ("Infrastructure Roadmap"); and develop a written plan for architecture development for the next six months			X
Develop a quarterly forecast of IT resource capacity requirements based on current and projected requirements (e.g., trends, monitored alerts, Projects, Service Request activity)			X
Work with Customer to evolve Customer's technology standards and provide architectural adjustment recommendations based on Customer's volume forecasts			X
Serve as coordinator of all infrastructure related activities impacting Virtustream during major customer initiatives. In this role the TAM will work with the respective project managers to ensure the infrastructure components meet the project time lines.			X
Responsible for capturing all reasonable Customer requests related to the infrastructure, services, processes, Virtustream portals, automation, or documentation provided by Virtustream, estimating the effort and executing them as long as the volume of work is compatible with the workload of one FTE. (examples: different types of reporting beyond that mentioned above, process changes, training)			X

Supporting Infrastructure

8.22 (E) SUPPORTING INFRASTRUCTURE

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

EMC Response: The customer may desire to use a dedicated MPLS circuit to direct connect its workload in the Virtustream cloud to the customer's secure network. In such cases, Virtustream provides colocation services for customers to bring the network termination equipment to the Virtustream data center and the cross connect into the Virtustream cloud environment. In other cases, the customer may need to place highly non-standard equipment in the Virtustream data center so that this specific equipment can work together with IaaS. In such cases, Virtustream provides colocation services with cross connect.

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

EMC Response: Generally, any installation in Virtustream's data center will be performed by Virtustream. Virtustream will invoice the customer for any installation charges.

Alignment of Cloud Computing Reference Architecture

8.23 (E) ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE

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

EMC Response: Virtustream's solution is fully NIST compliant for *Essential Characteristics*, as the Infrastructure as a Service (IaaS) *Service Model*, with all deployment options – Private Cloud, Community Cloud, Public and Hybrid Cloud. To that extent:

1. Virtustream IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP.

2. Virtustream IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, NetBond, etc.) which is growing rapidly as option for connecting cloud resources.

3. Key to Virtustream solution is its proprietary and patented solution of μVM technology, which is effectively a granular solution for resource pooling, providing application performance, pay for consumption only and segregate resources for security and compliance, but aggregate for cost efficiency. In addition, Virtustream is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and getting down to cluster and host machine level.

4. Virtustream's self-service portal, ticketing system and also the Technical Account Manager, who is the single point of contact for Participating Entities allows for provisioning and deprovisioning of resources and services. In addition, Virtustream is uniquely positioned to provide application level provisioning as part of its standard automation and orchestration tool.

5. The fundamental of Virtustream solution is based on µVM Technology, which is very unique in terms of billing. Virtustream solution takes average consumption of compute resources, and Participating Entities would only pay for actual resources based on a monthly average. This is in comparison with traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, consumer of the cloud pays, but when it is down, they don't. In case of the Virtustream solution, customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs; also, Virtustream can provide consultative and project support based on time and materials.

6. The deployment of Virtustream cloud can be on-premise or private based on purchase of its Cloud Management Platform, Community Cloud based on its IaaS, Public Cloud based on its IaaS and Hybrid cloud based on its ability to provide software and IaaS combined.

SECTION 7 – CONFIDENTIAL, PROTECTED OR PROPRIETARY INFORMATION

All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write "None" in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

EMC Response: None.

SECTION 8 – EXCEPTIONS AND/OR ADDITIONS TO THE STANDARD TERMS AND CONDITIONS

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations.

If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

EMC Response: In compliance with Section 3.4 of the RFP EMC is including exceptions and additions to the Master Agreement Terms and Conditions as part of our proposal. The exceptions and/or additions regarding the Master Agreement Terms and Conditions include a rationale for the specific requirement and recommended verbiage for the Lead State's consideration. The recommended changes to the verbiage are consistent in content, context and form with the Master Agreement Terms and Conditions.

We have limited our requested changes to those that are critical to EMC and the ultimate end-user customers. Our proposed changes include corrections to avoid ambiguity and the use of inconsistent terms and changes to more closely align with EMC's standard commercial terms. Specific terms and conditions were added to address areas not covered in the Master Agreement and to modify terms that are inconsistent with standard commercial practices.

EMC currently holds two NASPO ValuePoint Master Contracts. The terms and conditions of the current Master Contracts are substantially similar to the exceptions submitted for your consideration as part of our proposal. Due to the unique nature of the IaaS offer terms specific to IaaS have been included.

EMC believes the recommended changes to the verbiage and additional terms and conditions are fair and equitable to the Lead State, the Participating Entities and EMC. The terms agreed to in the Master Contract will allow expeditious negotiation of Participating Addenda. The recommended changes and additions are appropriate for the types of services offered. The additional terms are necessary to ensure that the Purchasing Entity fully understand the framework of the IaaS offer.

Our IaaS offerings have been designed to meet the needs of the commercial and government marketplaces. Modifications to standard terms and conditions included as exhibits to our Master Agreement exceptions may result in modifications of our standard commercial services and the associated fees.

EMC's proposal includes the redline version of Attachment A, Master Agreement and Exhibit 3 to Attachment A (IaaS) which we have provided as separate attachments to the technical proposal. The following exhibits have been incorporated into the Master Agreement as part of our exceptions and have also been provided as separate attachments to the technical proposal:

- Exhibit 4 Acceptable Use Policy
- Exhibit 5 Cloud Cover Services Service Description
- Exhibit 6 Cloud Platform Services Service Description

For the information we are providing as mentioned, please refer to the separately attached documents titled:

- "Attachment_A_-_NASPO_ValuePoint_Master_Agreement_Terms_and_Conditions_final 0303.docx"
- "Exhibit 3 to AttachmentA (IaaS)(2-24-16).docx"
- "Exhibit 4 Acceptable Use Policy.docx"
- "Exhibit 5 CCS Service Description NASPO 2016 March.docx"
- "Exhibit 6 CPS Service Description NASPO 2016 March.docx"

The contact information for person(s) that will be directly involved in the terms and conditions negotiations follows:

Joe Spaniol
8444 Westpark Dr., Suite 100
McLean, VA 22102
Office: 703-970-5161
Cell: (410) 991-1939
joe.spaniol@emc.com

Rita Roles
8444 Westpark Dr., Suite 100
McLean, VA 22102
Office: 703-907-5863
Cell: 703-334-1597
rita.roles@emc.com

Wayne Arden
4800 Montgomery Lane, Suite 110
Bethesda, MD 20814
Office: 240.752.7671
Cell: 301.529.9329
wayne.arden@virtustream.com

Virtustream Acceptable Use Policy

GENERALLY

Virtustream, Inc. ("Virtustream") has developed this Acceptable Use Policy ("AUP") with the goal of fostering the responsible use of Virtustream's infrastructure, networks, cloud-based offerings, systems, services, web sites, facilities and products (collectively, the "Virtustream Infrastructure and Services") by our customers and other users of the Virtustream Infrastructure and Services (collectively, "Users"), and to enable us to provide Users with secure and reliable services. By using the Virtustream Infrastructure and Services, Users consent to be bound by the terms of this AUP. Virtustream reserves the right to modify this AUP in its discretion at any time. Such modifications will be effective when posted and you are expected to check this page from time to time to take notice of any changes we make, as they are legally binding on you. Any use of the Virtustream Infrastructure and Services after such modification shall constitute acceptance of such modification. Some of the provisions contained in this AUP may also be superseded by provisions or notices published elsewhere on our web site or in any other contract between us.

SUSPENSION, TERMINATION

If Virtustream determines that any User has violated any element of this AUP, Virtustream may terminate or suspend its provision of the Virtustream Infrastructure and Services to that Usere. Virtustream will suspend service for violation of the AUP on the most limited basis as Virtustream determines is reasonably practical under the circumstances to address the underlying violation. Virtustream will attempt to notify User prior to suspending service for violation of the AUP (which may be via email or any other notification); provided, however, Virtustream may suspend service without notice if Virtustream becomes aware of a violation of any applicable law or regulation or activity, including but not limited to a violation of the AUP, that exposes Virtustream to criminal or civil liability or that exposes the Virtustream infrastructure, network or services or any third party property to harm. Such harm may include, but is not limited to, risk of having one or more IP addresses placed on blacklists. Virtustream may take such further action as Virtustream determines to be appropriate under the circumstances to eliminate or preclude repeat violations, and Virtustream shall not be liable for any damages of any nature suffered by any User or any third party resulting in whole or in part from Virtustream's exercise of its rights under this AUP, except that nothing in this AUP shall exclude or limit Virtustream's liability for death or personal injury caused by its negligence or any other liability that cannot be excluded or limited by law.

PROHIBITED CONDUCT

General

The Virtustream Infrastructure and Services must be used in a manner that is consistent with the intended purpose of the Virtustream Infrastructure and Services and may be used only for lawful purposes. Users shall not use the

Virtustream Infrastructure and Services in order to transmit, distribute or store content: (a) in violation of any applicable law or regulation, including export or encryption laws or regulations; (b) that may adversely affect the Virtustream Infrastructure and Services or other Virtustream customers; or (c) that may expose Virtustream to criminal or civil liability.

Inappropriate Content

Users shall not use the Virtustream Infrastructure and Services to transmit, distribute or store material that is inappropriate, as reasonably determined by Virtustream, or material that is obscene (including child pornography), defamatory, libelous, threatening, abusive, hateful, or excessively violent. Notwithstanding the foregoing or anything else to the contrary, no pornographic content of any kind may be stored (either permanently or temporarily), processed by or transmitted through any of Virtustream's cloud based services or any of Virtustream's cloud based infrastructure, including, without limitation, Virtustream's xStream platform.

Intellectual Property

Material accessible through or contained within the Virtustream Infrastructure and Services may be subject to protection under privacy, data protection or confidentiality laws and may contain intellectual property rights owned by Virtustream or third parties, including but not limited to, copyright, patents, trademarks, trade names, trade secrets or other proprietary information. Users shall not use the Virtustream Infrastructure and Services in any manner that would infringe, dilute, misappropriate, breach or otherwise violate any such rights or laws. Users are responsible for ensuring that all applications, software, programs, and content which are hosted though the Virtustream Infrastructure and Services are properly licensed from the applicable third parties to the extent required in the context of the applicable deployment. Users will indemnify in full, and keep fully indemnified on a continuing basis, Virtustream with respect to any claims by third parties brought against Virtustream based on an allegation that any such User failed to comply with its obligations under this paragraph.

Harmful Content

Users shall not use the Virtustream Infrastructure and Services to transmit, distribute or store material that may be harmful to or interfere with the Virtustream Infrastructure and Services or any third party's networks, systems, services, or web sites. Such prohibited harmful content includes, but is not limited to, viruses, worms, and Trojan horses.

Fraudulent/Misleading Content

Users shall not use the Virtustream Infrastructure and Services to transmit or distribute material containing fraudulent offers for goods or services, or any advertising or promotional materials that contain false, deceptive, or misleading statements, claims, or representations or which does not comply with any applicable advertising laws or codes of practice.

Collecting Information

Users shall not use the Virtustream Infrastructure and Services to store or collect, or attempt to store or collect, personal data (including data as defined in the Data Protection Directive (Directive 95/46/EC)) relating to any third parties without their prior knowledge and consent and Users must comply at all times with the Data Protection Directive and all other applicable data protection legislation.

Email and Unsolicited Messages

Users shall not use the Virtustream Infrastructure and Services to transmit unsolicited e-mail messages, including, without limitation, unsolicited bulk email ("spam"). Further, Users are prohibited from using the service of another provider to send spam to promote a website hosted on or connected to the Virtustream Infrastructure and Services. In addition, Users shall not use the Virtustream Infrastructure and Services in order to send e-mail messages which are excessive and/or intended to harass or annoy others.

Other Improper Actions

Users shall not use the Virtustream Infrastructure and Services to conduct activities that may be harmful to or interfere with the Virtustream Infrastructure and Services or any third party's networks, systems, services, or Web sites, including, but not limited to, flooding, mail bombing, or denial of service attacks. Users are prohibited from violating or attempting to violate the security of the Virtustream Infrastructure and Services or the computers, accounts, or networks of another party. Users are also prohibited from any activity considered a precursor to attempted security violations, including, but not limited to, any form of scanning, probing, or other testing or information gathering activity. Inappropriate activity may result in civil or criminal liability. Virtustream may investigate such activity, and may involve and cooperate with law enforcement authorities in prosecuting Users involved in such activity.

Responsibility for Content

Virtustream takes no responsibility for any content created or accessible on or through the Virtustream Infrastructure and Services. Virtustream is not obligated to monitor such content. Virtustream will not exercise any editorial control over such content. In the event that Virtustream becomes aware that any such content may violate this AUP and/or expose Virtustream to civil or criminal liability, Virtustream reserves the right to block access to such material and suspend or terminate its provision of the Virtustream Infrastructure and Services to any User creating, storing or disseminating such material. Virtustream further reserves the right to cooperate with legal authorities and third parties in any investigation of alleged wrongdoing.

Responsibility for End Users

Where agreed in Customer's contract with Virtustream, Customers may extend access to the Virtustream Infrastructure and Services to their end users. Where this is done, it is the Customer's responsibility to ensure that all of its end users comply with this AUP.

Reporting Violations

Virtustream requests that any person who becomes aware of a violation of this AUP reports this information to Virtustream by email to legal@virtustream.com. Virtustream may take any appropriate action as it reasonably deems fit in its sole discretion in respect of such violations.

EXHIBIT 5

CLOUD COVER SERVICES
SERVICE DESCRIPTION

1. SUPPORT SERVICES OVERVIEW

The Services available to be delivered pursuant to this SD are set forth below (the "Cloud Cover Services").

The SAP and Non SAP Cloud Cover Services available to be delivered:

1.1 Operating System Support

Operating System is available as an Onshore and Offshore service. One supported OS per VM.

Operating System Support			
CPT SKU	**Product Name**	**Description**	**Notes**
Onshore: CC-NS-ONOS-STD Offshore: CC-NS-OFOS-STD	**Standard** Operating System Support	• 24x7x365 monitoring of Customer's OS server environment and notification to Customer of threshold breaches. • Patching of Critical *Microsoft only* Operating System patches. • See schedule A.1 ("Standard Operating System Support") for details.	Charged per VM and billed monthly. For more information, see: **Schedule A:** Operating System Support **Appendix II:** CCS Service Desk **Appendix IV:** Patch Management **Appendix III:** Supported Systems
Onshore: CC-NS-ONOS-BUS Offshore: CC-NS-OFOS-BUS	**Business** Operating System Support	• 24x7x365 monitoring of Customer's OS server environment and notification to Customer of threshold breaches. • Monday – Friday 8:00 AM EST to 6:00 PM EST incident resolution and responses to Service Requests. • Capacity Management. • Operating System Management. • Patch Management. • See schedule A.2 ("Business Operating System Support") for details.	
Onshore: CC-NS-ONOS-ENT Offshore: CC-NS-OFOS-ENT	**Enterprise** Operating System Support	• 24x7x365 monitoring of Customer's OS server environment and notification to Customer of threshold breaches. • 24x7x365 incident resolution. • Monday – Friday 8:00 AM EST to 6:00 PM EST responses to Service Requests. • Capacity Management. • Operating System Management. • Patch Management. • See schedule A.3 ("Enterprise Operating System Support") for details.	

1.2 Database Support

Operating System and Database Support is available as an Onshore and Offshore service. Maximum two databases and one OS per VM.

Database & Operating System Support			
CPT SKU	**Product Name**	**Description**	**Notes**
Onshore: CC-NS-ONDB-STD Offshore: CC-NS-OFDB-STD	**Standard** Operating System and Database Support	• 24x7x365 monitoring of Customer's OS and RDBMS server environment and notification to Customer of threshold breaches. • Patching of Critical *Microsoft only* Operating System patches. • See schedule B.1 ("Standard Database Support") for details.	Charged per instance and billed monthly. For more information, see: **Schedule B:** Database Support **Appendix II:** CCS Service Desk **Appendix IV:** Patch Management **Appendix III:** Supported Systems
Onshore: CC-NS-ONDB-BUS Offshore: CC-NS-OFDB-BUS	**Business** Operating System and Database Support	• 24x7x365 monitoring of Customer's OS and RDBMS server environment and notification to Customer of threshold breaches. • Monday – Friday 8:00 AM EST to 6:00 PM EST incident resolution and responses to service requests. • Capacity Management. • Database Management. • Operating System Management. • Patch Management for Operating Systems, Critical Patches for RDBMS. • See schedule B.2 ("Business Database Support") for details.	

Onshore: CC-NS-ONDB-ENT	**Enterprise** Operating System and Database Support	• 24x7x365 monitoring of Customer's OS and RDBMS server environment and notification to Customer of threshold breaches. • 24x7x365 incident resolution, Monday – Friday 8:00 AM EST to 6:00 PM EST responses to Service Requests. • Capacity Management. • Database Management. • Operating System Management. • Patch Management for Operating Systems, Critical Patches for RDBMS. • See schedule B.3 ("Enterprise Database Support") for details.	
Offshore: CC-NS-OFDB-ENT			

1.3 SAP Support

The 3 tiers of SAP Support apply to Onshore and Offshore Services as well as production and non-production instances. Maximum two databases and one OS per VM.

SAP Support			
CPT SKU	**Product Name**	**Description**	**Notes**
Non-Prod: CC-SAP-ONNH-STD Prod: CC-SAP-ONPH-STD	Onshore **Standard** SAP Technical Support (HANA/Non-HANA)	• 24x7x365 monitoring of Customer's SAP environment and notification to Customer of threshold breaches. • See schedule C.1 ("Standard SAP Support") for details.	Onshore SAP technical support includes HANA. HANA support is not available offshore.
Non-Prod: CC-SAP-ONNH-BUS Prod: CC-SAP-ONPH-BUS	Onshore **Business** SAP Technical Support (Basis, HANA/Non-HANA)	• 24x7x365 monitoring of Customer's OS and RDBMS (Including HANA) server environment and notification to Customer of threshold breaches. • Monday – Friday 8:00 AM EST to 6:00 PM EST incident resolution and responses to service requests. • SAP Basis Management. • Database Management. • Operating System Management. • Patch Management for SAP, Databases, and Operating Systems. • See schedule C.2 ("Business SAP Support") for details.	Charged **Per single SAP VM Standalone Instance** and billed monthly. For example: An ECC instance with 1 CI and 2 app servers would require
Non-Prod: CC-SAP-ONNH-ENT Prod: CC-SAP-ONPH-ENT	Onshore **Enterprise** SAP Technical Support (Basis, HANA/Non-HANA)	• 24x7x365 monitoring of Customer's OS and RDBMS (Including HANA) server environment and notification to Customer of threshold breaches. • 24x7x365 incident resolution, Monday – Friday 8:00 AM EST to 6:00 PM EST responses to Service Requests. • SAP Management. • Database Management. • Operating System Management. • Patch Management for SAP, Databases, and Operating Systems. • See schedule C.3 ("Enterprise SAP Support") for details.	1 CCS SAP support 2 CCS OS support (additional VMs within an SAP instance only require OS support)
Non-Prod: CC-SAP-OFNS-STD Prod: CC-SAP-OFPS-STD	Offshore **Standard** SAP Technical Support	• 24x7x365 monitoring of Customer's SAP environment and notification to Customer of threshold breaches. See schedule C.1 ("Standard SAP Support") for details.	
Non-Prod: CC-SAP-OFNS-BUS Prod: CC-SAP-OFPS-BUS	Offshore **Business** SAP Technical Support (Basis/Non-HANA)	• 24x7x365 monitoring of Customer's OS and RDBMS (**Not** Including HANA) server environment and notification to Customer of threshold breaches. • Monday – Friday 8:00 AM EST to 6:00 PM EST incident resolution and responses to service requests. • SAP Basis Management. • Database Management. • Operating System Management. • Patch Management for SAP, Databases, and Operating Systems. See schedule C.2 ("Business SAP Support") for details.	For more information, see: **Schedule C:** SAP support **Appendix II:** CCS Service Desk **Appendix III:** Supported Systems **Appendix IV:** Patch Management

Non-Prod: CC-SAP-OFNS-ENT Prod: CC-SAP-OFPS-ENT	Offshore **Enterprise** SAP Technical Support (Basis/Non-HANA)	• 24x7x365 monitoring of Customer's OS and RDBMS (**Not** Including HANA) server environment and notification to Customer of threshold breaches. • 24x7x365 incident resolution, Monday – Friday 8:00 AM EST to 6:00 PM EST responses to Service Requests. • SAP Management. • Database Management. • Operating System Management. • Patch Management for SAP, Databases, and Operating Systems. See schedule C.3 ("Enterprise SAP Support") for details.	HA
Onshore: CC-SAP-ONUS-CCS Offshore: CC-SAP-OFUS-CCS	SAP User and Security Administration and Change Management Support		
Offshore: CC-SVC-OFBO-ADM	SAP BODS Administrator	Covers up to 12 instances	Charged as a monthly service or hourly professional service billed monthly. Only available Offshore

1.4 Cloud Cover Setup

Cloud Cover Setup is currently only available as an Onshore Service. SAP User, Security, and Change Management Process Setup is available both Onshore and Offshore.

Cloud Cover			
Product ID	**Product Name**	**Description**	**Notes**
CC-SVC-ONCC-1T	Cloud Cover Setup	Cloud Cover Setup fee. Customer will be charged for each VM set up. This covers the setup of the monitoring infrastructure, working with Customer on a monitoring solution, and tuning the monitoring threshold before the solution goes into production.	Charged per VM and billed monthly.
Onshore: CC-SAP-ONUS-1T Offshore: CC-SAP-OFUS-1T	SAP User and Security Administration and Change Management Support Setup		

1.5 Technical Account Management Services (TAMS)

Technical Account Manager			
Product ID	**Product Name**	**Description**	**Notes**
CC-TAM-TAM-PLAT CC-TAM-TAM-GOLD CC-TAM-TAM-SILV CC-TAM-TAM-INST	Technical Account Manager (TAM)	TAM is a customer account based service based on size and complexity of the Customer solution. TAM will coordinate day-to-day operation, service level management and SL reporting. This service is to be part of Virtustream offering (as further specified in a PO Agreement).	Available in silver, gold, platinum, instance based, or as Ad Hoc sub services. For more information, see: Section 6: Technical Account Management Services (TAM)

2. ASSUMPTIONS

The pricing, timing, and other terms of this SD with respect to the performance of the Services are dependent on the following assumptions being valid:

a. The Customer fulfills the responsibilities specified in this SD or reasonably requested by Virtustream.

b. The Customer will respond promptly, to any Virtustream requests to provide direction, information, approvals or decisions that are reasonably necessary to be provided by the Customer for Virtustream to perform the Services.

c. The Customer will ensure that all nominated Customer personnel who work on Virtustream's systems or equipment are adequately qualified and receive suitable training at Customer's expense both to ensure the safety of the Customer's personnel and to safeguard Virtustream's systems or equipment.

d. Customer shall obtain all necessary licenses and permissions to use third party software for the provision of the Services and where necessary access to the software, data and other materials and modifications for the purposes of the provision of the Services.

e. Customer shall ensure that it obtains all rights and permissions from vendors and other third parties as necessary to permit Virtustream to access the information and data to be made available to Virtustream as specified hereunder.

3. CHANGE CONTROL PROCEDURES; THIRD PARTY MATERIALS

3.1 Notice of Changes

Virtustream will give Customer advance notice of any changes being applied to Services that may affect the Customer in accordance with Virtustream's change management procedures. Notices of changes are disseminated by Virtustream through means of electronic mail distribution lists and other appropriate media as determined by Virtustream. If emergency maintenance is required due to an Incident, Virtustream will give the Customer notice as is reasonably possible, without impeding the resolution of the Incident.

3.2 Third Party Materials

Virtustream may provide assistance with Customer's procurement of third-party hardware, software and other items specified in this SD ("Third Party Materials"). Virtustream makes no express or implied warranties of any kind with respect to such Third Party Materials. Virtustream shall have no liability to Customer, or any other party, for any loss, claim or damage of any nature caused or alleged to be caused directly or indirectly, incidentally or consequentially by the Third Party Materials, any inadequacy thereof, deficiency or defect therein, whether in strict liability or otherwise, in any way related or arising out of this SD, and whether or not advised of the possibility of any such losses or damages.

4. DEFINITIONS

All capitalized terms used but not defined in this Service Description shall have the same meaning as those set out in the Master Service Agreement or as set forth below.

Capacity Management: a process used by Virtustream to manage information and gather Customer data related to Customer's present and past technology (IT) to assess Customer's IT capacity needs.

Database System: the combination of a database, a database management system and a data model.

Incident: an event which is not part of the standard operation of a Service and which causes or may cause disruption to or a reduction in the quality of Services.

Instance: (For SAP) One or more Virtual Machines assembled to run a single tier of an SAP environment (e.g. PRD = 3 VMs: a Central Instance, DB, and APP. These VMs together constitute 1 instance).

Microsoft Vulnerability Severity Ratings: see http://technet.microsoft.com/en-us/security/gg309177.aspx

Notification: Customer creates a ticket or a monitoring event is validated by Virtustream.

Offshore: a portion of the labor required to deliver the service is sourced from outside the United States.

Onshore: all labor require to deliver the service is sourced from within the United States.

Problem: an Incident that was temporarily resolved but requires further work to permanently resolve and often includes recurring incidents or incidents which are classified as high priority (P1) or for which Customer requests a Root Cause Analysis or problem review through TAM.

Relational Database Management System: a program that allows the creation, updating and administration of a relation database.

Response (and its derivatives): Virtustream has acknowledged to Customer (via email or telephone) the occurrence of the Incident. The Response time shall be measured from the time Customer creates a ticket by contacting the Service Desk or a monitoring event is validated to Virtustream's acknowledgement via the Service Desk.

Restore: the restoration of Services as defined by agreed-to Service Levels (which may include by workaround or other alternative means) in a manner acceptable to Customer in its reasonable discretion. Measured from the earlier of (1) discovery of the Incident by Virtustream or (2) the time when the Incident call, message or report is received by Virtustream from Customer or Customer's or Virtustream's personnel.

Root Cause Analysis: the formal process, documented in writing by Virtustream and approved by Customer, to be used by Virtustream to diagnose problems at the lowest reasonable level which includes a report of the corrective action to be taken and defined timelines for corrective actions, which shall eliminate, to the extent reasonably possible, repeat failures.

7

Service Monitoring: a process used by Virtustream to monitor a defined service for availability and performance.

Service Request: requests for information, advice, standard changes, normal changes, or access to a service, within the Services set out in this SD.

5. SERVICE LEVELS

5.1 Commencement of Service Levels specified in Section 5 ("Service Levels").

Commencing thirty (30) days from the Service Date, Virtustream's performance of the Services will meet each applicable Service Level. If Virtustream's performance of the Services does not meet the applicable Service Level, then Virtustream will promptly restore its performance to meet such Service Level. Additionally, after restoring service or otherwise resolving any immediate problem as specified in this Service Description, if Virtustream fails to provide Services in accordance with the Service Levels, Virtustream shall:

a. Promptly investigate and report on the causes of such problem;

b. Provide a Root Cause Analysis of such failure as soon as practical after such failure or at Customer's request;

c. Correct such problem that is Virtustream's fault or responsibility, as soon as practical and coordinate the correction of such problem if Virtustream does not have responsibility for the cause of such problem (that is Virtustream's fault or responsibility);

d. Advise Customer of the status of remedial efforts being undertaken with respect to such problem;

e. Demonstrate to Customer's reasonable satisfaction that the causes of such problem (that is Virtustream's fault or responsibility) have been or shall be corrected on a permanent basis; and

f. Take corrective actions to prevent any recurrence of such problem (that is Virtustream's fault or responsibility).

Promptly following Virtustream's failure to meet a Service Level, Virtustream will perform a root cause analysis to determine the reason for that failure. Upon Virtustream's determination of the cause of such failure, it will provide to Customer a preliminary report citing the cause of such failure. If Virtustream determines that the failure was due to Virtustream, an additional report will be provided that details the root causes of the failure, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. Virtustream will correct the problem and use reasonable commercial efforts to minimize the re-occurrence of such failures.

5.2 Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

i. A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

ii. Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);

iii. Any hardware, software or other product of a third-party or Customer equipment;

iv. Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;

v. Downtimes resulting from a Virtustream's scheduled maintenance windows;

9

vi. Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;

vii. Viruses; provided that the infected system had virus protection for which the virus protection software updates were up to date; and

viii. Customer has elected to purchase a base commitment that is not sufficient to run Customer's system.

5.3 Service Desk Response Times

Subject to any Service Level Exception, Virtustream will respond to an Incident within the Response time set forth below 95% of the time.

Priority	Response Time
Priority 1	Within 30 minutes of Notification
Priority 2	Within 60 minutes of Notification
Priority 3	Within 4 hours of Notification
Priority 4	Within 1 business day of Notification

See appendix II.6.3 ("Incident Prioritization") for definitions of priority levels.

5.4 Service Level Credits

5.4.1 Credit Schedule

Virtustream will pay service level credits only when it has direct and full responsibility for any failure to meet the SAP Application Availability Service Level ("Service Level Failure") provided that the Customer is utilizing Virtustream's SAP Application Cloud Cover Services Subject to any Service Level Exception, Virtustream will provide to Customer a service level credit (excluding expenses) for any month in which there is Service Level Failure as follows:

SAP Application Availability Production	Service Level Credit: percentage of applicable Cloud Cover monthly fees under the affected monthly invoice
99.90% -99.94%	1%
99.75% -99.89%	3%
99.65% -99.74%	5%
99.50% - 99.64%	7%
99.30% - 99.49%	10%
below 99.29%	15%

SAP Application Availability Non-Production	Service Level Credit: percentage of applicable Cloud Cover monthly fees under the affected monthly invoice
99.1% - 99.4%	1%
98.7% - 99.09%	3%
98.3% - 98.69%	5%

10

97.9% - 98.29%	7%
97.5% - 97.89%	10%
below 97.49%	15%

Exemption to Incident Response times include lack of email or telephone availability.

% of all Incident responses achieving response times	Service Level Credit: percentage of applicable Cloud Cover monthly fees under the affected monthly invoice
92.5% -94.99%	1%
90.0% -92.49%	2%
85.00% -89.99%	3%
below 85%	5%

5.4.2 Form and Limitations of Credit

Service Level Credits shall constitute liquidated damages which are believed by the parties to be reasonably indicative of the damages incurred by Customer, and shall be Customer's sole and exclusive remedy for Virtustream's Service Level Failure. Where a single incident results in more than one Service Level Failure, Virtustream will provide Customer with only the largest Service Level Credit. Customer will not be entitled to Service Level Credits for each of such Service Level Failures.

Virtustream may, at its option, pay the Service Level Credit to Customer or give Customer a credit against the charges otherwise payable to Virtustream, on the next invoice with respect thereto.   If the Customer's accounts receivable balance is not current in the month in which the Service Level Failure occurred (i.e. the Customer has not paid the its invoices in accordance with the terms of the Master Services Agreement, the Customer shall not be entitled to a Service Level Credit, and Virtustream will be excused for its failure to meet or exceed the Service Levels.

In no event will the aggregate Service Level Credits in any month exceed 15% of the total fees payable for such month pursuant to the applicable Order Form.

6. TECHNICAL ACCOUNT MANAGEMENT SERVICES (TAMS)

Technical Account Management Services (TAMS) is a customer account based service based on size and complexity of the Customer solution. The Technical Account Manager (TAM) will coordinate day-to-day operation, service level management and reporting, capacity management, and other services associated with managing Cloud Cover Services. Customer can choose one of three levels of TAM: Silver (operations management), Gold (single point of contact for mission critical activities & quarterly reviews), and Platinum TAM (strategic partnership). The TAM will be available from 8AM – 5PM ET and outside of these hours by pre-arrangement.

6.1 TAM Services
6.1.1 Primary TAM Services
The primary TAM Services available to be delivered:

Product ID	Product Name	Description	Notes
TAM Services			
CC-TAM-TAM-PLAT	Technical Account Manager (TAM) – Platinum Ea	TAM is a customer account based service based on size and complexity of the Customer solution. TAM will coordinate day-to-day operation, service level management and SL reporting. This service is to be part of Virtustream offering (as further specified in a PO Agreement).	"Strategic Partnership"
CC-TAM-TAM-GOLD	Technical Account Manager (TAM) – Gold Ea		"Single Point of Contact for Mission Critical Activities & Quarterly Reviews"
CC-TAM-TAM-SILV	Technical Account Manager (TAM) – Silver Ea		"Operations Management"
CC-TAM-TAM-INST	Technical Account Manager (TAM) – Per Instance		

The table below specifies the responsibilities of and/or the services to be provided by the TAM.

Definition	Silver TAM	Gold TAM	Platinum TAM
Operations Management (Weekly and Monthly)			
SLA Management / Compliance / Reporting	X	X	X
Contract management	X	X	X
Proactive Statistical Analysis of Performance Data with recommendations to optimize performance and utilization (Rightsizing)	X	X	X
Best Practice recommendations and Run Optimization	X	X	X
Status Reporting (Weekly Checkpoint Meeting)	X	X	X
Respond to Customer question / handle Customer escalation requests	X	X	X
Incident Management & Central Coordination	X	X	X
Point of contact for requests for RCA	X	X	X
Facilitate Problem Management meeting with Customer to review RCA reports (as	X	X	X

needed)			
Track and report on Incident and Service Request ticket aging; facilitate prompt completion of any tickets aging beyond SLOs	X	X	X
Single Point of Contact for Mission Critical Activities & Quarterly Reviews			
Monitor the Services and proactively work with Customer to identify ongoing IT resource capacity *NOTE: Consumption will be part of the Monthly billing.*		X	X
Execute provisioning tasks from customer requests		X	X
Failover, D/R testing coordination		X	X
Operations Integration with Customer Processes (example: customer Change Management attendance)		X	X
Quarterly Business review		X	X
For contracted services, perform quarterly reviews of reliability and availability using: Service Level reporting; Service management statistics; Resource usage and trending; Project execution; Capacity management and trending; Root Cause Analyses; Event history in the ITSM System; Customer satisfaction data; Security Event history and trending; Disaster recovery plans;		X	X
For Managed Services Platforms, perform a quarterly review of reliability and availability of the components of the Managed Services Platforms		X	X
Upon the completion of reviews, meet with Customer to propose improvements		X	X
Provide monthly reporting on service delivery (summary report of incident tickets & service requests including type, priority, min/mean/max time to complete, etc)		X	X
Provide copies of all run books to Customer and facilitate completion/updates for any run books and/or requested design documents		X	X
Strategic Partnership			
Access ongoing co-innovation and co-value realization			X
Strategic Roadmap and planning activities			X
Executive Scorecards			X
Brief Customer semi-annually on technology and process evolutions that may be of interest or beneficial to Customer			X
Assist Customer's BDPs and TDPs process such as providing: Specific, short-term steps and schedules for projects or changes expected to occur within the first twelve (12) months of each plan; Budgetary cost estimates to complete such projects; Reviews of Customer's business cases; Future volume projections, technology, and geographic changes that could impact Customer's systems and technical architectures			X
Facilitate quarterly demand management planning meetings			X

			X
Conduct semi-annual Infrastructure architecture planning sessions with Customer to review Customer's current business objectives and related technology demands; discuss the current market view of relevant technologies, IT industry trends, and architecture approaches; document and update a three (3) year infrastructure roadmap and implementation plan ("Infrastructure Roadmap"); and develop a written plan for architecture development for the next six months			X
Develop a quarterly forecast of IT resource capacity requirements based on current and projected requirements (e.g., trends, monitored alerts, Projects, Service Request activity)			X
Work with Customer to evolve Customer's technology standards and provide architectural adjustment recommendations based on Customer's volume forecasts			X
Serve as coordinator of all infrastructure related activities impacting Virtustream during major customer initiatives. In this role the TAM will work with the respective project managers to ensure the infrastructure components meet the project time lines.			X
Responsible for capturing all reasonable Customer requests related to the infrastructure, services, processes, Virtustream portals, automation, or documentation provided by Virtustream, estimating the effort and executing them as long as the volume of work is compatible with the workload of one FTE. (examples: different types of reporting beyond that mentioned above, process changes, training)			X

6.1.2 TAM Sub Services

The following Services are included in Platinum TAMS and can also be purchased as an individual service

Product ID	Product Name	Notes
CC-TAM-SLAR-1Y	SLA Review	Available as 1 year or monthly Service
CC-TAM-RP-1Y	Resource and Performance	Available as 1 year or monthly Service
CC-TAM-WSIR-1Y	Weekly Status and Incident Reporting	Available as 1 year or monthly Service
CC-TAM-RBR-1Y	Reporting and Business Review	Available as 1 year or monthly Service
CC-TAM-CIR-1Y	Co-Innovation Roundtables	Available as 1 year or 6 month Service
CC-TAM-ES-1Y	Executive Scorecards	Available as 1 year or 3 month Service
CC-TAM-DMM-1Y	Demand Management Meetings	Available as 1 year or 3 month Service
CC-TAM-ITRF-1Y	IT Resource Forecast	Available as 1 year or 3 month Service
CC-TAM-IMSD-1Y	Incident Management / Service Delivery	available as 1 year service
CC-TAM-OPIN-1Y	Operational Integration	available as 1 year service
CC-TAM-IAP-PROJ	Infrastructure Architecture Planning	Project Based
CC-TAM-DR-PROJ	Disaster Recovery	Project Based
CC-TAM-PBD-PROJ	Process and Build Documentation	Project Based
CC-TAM-CM-PROJ	Contract Management	Project Based
CC-TAM-PI-PROJ	BDP/TDP Process Involvement	Project Based
CC-TAM-SRP-PROJ	Strategic Roadmap and Planning	Project Based
CC-TAM-RTS-PROJ	Review/Improve Technology Standards	Project Based

CC-TAM-ISC-PROJ	VS Infrastructure & Service Coordination	

6.2 Operating System and Database Monitoring

The following Monitoring Services can be requested through TAM:

Service Code	Service Name	Service Description
AVM004	System Usage/Utilization	Monitor system performance counters such as CPU and Memory utilization, disk I/O, and network I/O.

6.3 Capacity Management

Virtustream will provide Capacity Management Services via TAM, whereby Virtustream will collect the data monitored as part of proactive monitoring. Automated Capacity Management is included with

Service Code	Service Name	Service Description
CPM001	Capacity Report	Summarized report of a predefined period to aid in Capacity Management. Available on demand

Operating System and Database Support.

SCHEDULE A- OPERATING SYSTEM SUPPORT

A.1 Standard Operating System Support

Overview for Standard Operating System Support		
Section	Service	Frequency
A.1.1	Monitoring	24x7x365
A.1.2	Notification	
	Capacity Management	Not included
II.1.1	Responses to Incidents	
II.1.2	Responses to Service Requests	
	Operating System Management	
A.1.3	Patch Management (Critical Patches for Microsoft OS only)	Monthly

Operating System support includes one supported Operating System per VM. See appendix III.1 ("Operating Systems") for supported operating systems.

A.1.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream will monitor event behavior in such a way that it can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

A.1.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

For Standard Support, alerts will be sent automatically, without Virtustream checking for false positives. Alerts will not automatically trigger the creation of a ticket in the service desk. Customer may create a ticket and request that Virtustream assist in resolving an issue. Customer will be charged at Virtustream's current time and material rates.

The default Notification settings for Operating Systems are described in the table below:

16

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

A.1.3 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Standard Operating System Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM003	Critical Patches	Implementation of Critical and/or Security Patches for supported **Microsoft** OS.	Monthly

With Standard Support, Patches will be released to Customer's production environment without prior testing in Customer's QA environment.

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

A.2 Business Operating System Support

Overview for Business Operating System Support		
Section	Service	Frequency
A.2.1	**Monitoring**	**24x7x365**
A.2.2	**Notification**	
A.2.3	**Capacity Management**	**Quarterly**
II.1.1	**Responses to Service Requests**	**Monday-Friday,** **8 AM EST- 5 PM EST.**
II.1.2	**Responses to Incidents**	
A.2.4	**Operating System Management**	
A.2.5	**Patch Management**	**Monthly**

Operating System support includes one supported Operating System per VM. See appendix III.1 ("Operating Systems") for supported operating systems.

A.2.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

A.2.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. Major and Critical Alerts will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST.

The default Notification settings for Operating Systems are described in the table below:

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 5 mins

A.2.3 Capacity Management

Virtustream will provide Capacity Management Services, whereby Virtustream will collect the data

Service Code	Service Name	Service Description
CPM001	Capacity Report	Summarized report of a predefined period to aid in Capacity Management. Available on demand

monitored as part of proactive monitoring.

More comprehensive Capacity Management Services can be purchased through TAM (see section 6 "Technical Account Management Services (TAMS)").

A.2.4 Operating System Management

Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur when managing an operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description

OSM001	Storage and File Management	Create/delete/change file systems, build new virtual machines.
OSM002	User and Profile Management	Create/Delete/Change operating system users. profiles and policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, or via Capacity Management or Service Monitoring.
OSM005	Housekeeping	Create/delete/change vendor specific housekeeping best practices.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management Services and the roles of Customer and Virtustream.

A.2.5 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Business Operating System Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM002	OS patches and hotfix	Implementation of supported OS patches (non-security), as well as hotfixes.	Monthly
PMM003	Critical Patches	Implementation of Critical and/or Security Patches.	Monthly

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

A.3 Enterprise Operating System Support

Overview for Enterprise Operating System Support		
Section	Service	Frequency
A.3.1	**Monitoring**	**24x7x365**
A.3.2	**Notification**	
A.3.3	**Capacity Management**	**Quarterly**
II.1.1	**Responses to Incidents**	**24x7x365**
II.1.2	**Responses to Service Requests**	**Monday-Friday, 8 AM EST- 5 PM EST.**
A.3.4	**Operating System Management**	
A.3.5	**Patch Management**	**Monthly**

Operating System support includes one supported Operating System per VM. See appendix III.1 ("Operating Systems") for supported operating systems.

A.3.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time.
Virtustream will monitor event behavior in such a way that they can be proactive, identifying problems

and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

A.3.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. A Major Alert will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST. A Critical Alert will be escalated 24x7x365.

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		5 mins

The default Notification settings for Operating Systems are described in the table below:

A.3.3 Capacity Management
Virtustream will provide Capacity Management Services, whereby Virtustream will collect the data

Service Code	Service Name	Service Description
CPM001	Capacity Report	Summarized report of a predefined period to aid in Capacity Management. Quarterly on request.

monitored as part of proactive monitoring.

More comprehensive Capacity Management Services can be purchased through TAM (see section 6 "Technical Account Management Services (TAM)").

A.3.4 Operating System Management
Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur

when managing an operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description
OSM001	Storage and File Management	Create/delete/change file systems, build new virtual machines.
OSM002	User and Profile Management	Create/Delete/Change operating system users. profiles and policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, or via Capacity Management or Service Monitoring.
OSM005	Housekeeping	Create/delete/change vendor specific housekeeping best practices.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management services and the roles of Customer and Virtustream.

A.3.5 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Enterprise Operating System Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM002	OS patches and hotfix	Implementation of supported OS patches (non-security), as well as hotfixes.	Monthly
PMM003	Critical Patches	Implementation of Critical and/or Security Patches.	Monthly

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

SCHEDULE B- DATABASE SUPPORT

B.1 Standard Database Support

Overview for Standard Database Support		
Section	**Service**	**Frequency**
B.1.1	**Monitoring**	**24x7x365**
B.1.2	**Notification**	
	Capacity Management	**Not included**
II.1.1	**Responses to Incidents**	
II.1.2	**Responses to Service Requests**	
	Database Management	
	Operating System Management	
B.1.3	**Patch Management (Critical Patches for Microsoft OS only)**	**Monthly**

Database support includes up to 2 databases and 1 operating system per VM. See appendix III.1 ("Operating Systems") and appendix III.2 ("Relational Database Management Systems") for supported systems.

B.1.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

B.1.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

For Standard Support, alerts will be sent automatically, without Virtustream checking for false positives. Alerts will not automatically trigger the creation of a ticket in the service desk. Customer may create a ticket and request that Virtustream assist in resolving an issue. Customer will be charged at Virtustream's current time and material rates.

The default Notification settings for Database Systems are described in the table below:

22

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The most common default monitoring settings for databases are described in the table below:

Monitor	Notes	Default Threshold/ Value	Alert
Database Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any database resources.	This number should be "0" or "0" % wait time.	critical

B.1.3 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Standard Database and Operating System Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM003	Critical Patches	Implementation of Critical and/or Security Patches for supported **Microsoft** OS.	Monthly

With Standard Support, patches will be released to Customer's production environment without prior testing in Customer's QA environment.

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

B.2 Business Database Support

Overview for Business Database Support		
Section	**Service**	**Frequency**
B.2.1	**Monitoring**	**24x7x365**
B.2.2	**Notification**	
B.2.3	**Capacity Management**	**Quarterly**
II.1.1	**Responses to Service Requests**	**Monday-Friday, 8 AM EST- 5 PM EST.**
II.1.2	**Responses to Incidents**	
B.2.4	**Database Management**	
B.2.5	**Operating System Management**	
B.2.6	**Patch Management**	**Monthly**

Database support includes up to 2 databases and 1 operating system per VM. See appendix III.1 ("Operating Systems") and appendix III.2 ("Relational Database Management Systems") for supported systems.

B.2.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

B.2.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. A Major Alert will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST (for Business and Enterprise Support). A Critical Alert will be escalated 24x7x365 (for Enterprise Support).

The default Notification settings for Operating Systems are described in the table below:

24

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The most common default monitoring settings for databases are described in the table below:

Monitor	Notes	Default Threshold/Value	Alert
Database Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any database resources.	This number should be "0" or "0" % wait time.	critical

B.2.3 Capacity Management

Virtustream will provide Capacity Management Services, whereby Virtustream will collect the data

Service Code	Service Name	Service Description
CPM001	Capacity Report	Summarized report of a predefined period to aid in Capacity Management. Quarterly on request.

monitored as part of proactive monitoring.

More comprehensive Capacity Management Services can be purchased through TAM (see section 6 "Technical Account Management Services (TAMS)").

B.2.4 Database Management

Virtustream will provide "Database Management Services", which includes the day-to-day technical administration of the Database Systems. The Service will meet certain functions that occur when managing Relational Database Management Systems. The Database Management Services include the following:

Service Code	Service Name	Service Description
DMB001	Space Management	Manage all aspects of RDBMS space management for stability and availability of the RDBMS.
DMB002	Security Management	Implement security recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DMB003	Object Management	Manage all aspects of RDBMS object management for stability and availability of the system.
DMB004	Configuration Management	Implement configuration recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DMB005	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.
DMB006	RDBMS Backup	Initiate RDBMS backup tasks through RDBMS tools. Customer must purchase Backup Storage Service
DMB007	RDBMS Restore and Recovery Advice	Advice on Restore/recovery of supported RDBMS. Customer must purchase Backup Storage Service. Combined maximum of 2 service requests per month
DMB008	RDBMS Recovery	Perform recovery of supported RDBMS Systems. A combined maximum of 2 test Restore requests per month. Excludes recovery testing which would be at an additional cost. Customer must purchase Backup Storage Service

See RACI chart in appendix I.5 ("RACI for Database Management") for more information about Database Management services and the roles of Customer and Virtustream.

B.2.5 Operating System Management

Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur when managing an operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description
OSM001	Storage and File Management	Create/delete/change file systems, build new virtual machines.
OSM002	User and	Create/Delete/Change operating system users. profiles and

	Profile Management	policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, or via Capacity Management or Service Monitoring.
OSM005	Housekeeping	Create/delete/change vendor specific housekeeping best practices.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management services and the roles of Customer and Virtustream.

B.2.6 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Business Database and Operating System Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM002	OS patches and hotfix	Implementation of supported OS patches (non-security), as well as hotfixes.	Monthly
PMM003	Critical Patches	Implementation of Critical and/or Security Patches.	Monthly

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

B.3 Enterprise Database Support

Overview for Enterprise Database Support		
Section	Service	Frequency
B.3.1	**Monitoring**	**24x7x365**
B.3.2	**Notification**	
B.3.3	**Capacity Management**	**Quarterly**
II.1.1	**Responses to Incidents**	**24x7x365**
II.1.2	**Responses to Service Requests**	**Monday-Friday, 8 AM EST- 5 PM EST.**
B.3.4	**Database Management**	
B.3.5	**Operating System Management**	
B.3.6	**Patch Management**	**Monthly**

Database support includes up to 2 databases and 1 operating system per VM. See appendix III.1 ("Operating Systems") and appendix III.2 ("Relational Database Management Systems") for supported systems.

B.3.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time.

Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

B.3.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. A Major Alert will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST (for Business and Enterprise Support). A Critical Alert will be escalated 24x7x365 (for Enterprise Support).

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The default Notification settings for Operating Systems are described in the table below:

The most common default monitoring settings for databases are described in the table below:

Monitor	Notes	Default Threshold/Value	Alert
Database Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk	95%	major

		80%	major
	access.		
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any database resources.	This number should be "0" or "0" % wait time.	critical

B.3.3 Capacity Management

Virtustream will provide Capacity Management Services, whereby Virtustream will collect the data

Service Code	Service Name	Service Description
CPM001	Capacity Report	Summarized report of a predefined period to aid in Capacity Management. Quarterly on request.

monitored as part of proactive monitoring.

More comprehensive Capacity Management Services can be purchased through TAM (see section 6 "Technical Account Management Services (TAMS)").

B.3.4 Database Management

Virtustream will provide "Database Management Services", which includes the day-to-day technical administration of the Database Systems. The Service will meet certain functions that occur when managing Relational Database Management Systems. The Database Management Services include the following:

Service Code	Service Name	Service Description
DMB001	Space Management	Manage all aspects of RDBMS space management for stability and availability of the RDBMS.
DMB002	Security Management	Implement security recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DMB003	Object Management	Manage all aspects of RDBMS object management for stability and availability of the system.
DMB004	Configuration Management	Implement configuration recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DMB005	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.
DMB006	RDBMS Backup	Initiate RDBMS backup tasks through RDBMS tools. Customer must purchase Backup Storage Service
DMB007	RDBMS Restore and Recovery Advice	Advice on Restore/recovery of supported RDBMS. Customer must purchase Backup Storage Service. Combined maximum of 2 service requests per month
DMB008	RDBMS	Perform recovery of supported RDBMS Systems. A combined

Service Code	Service Name	Service Description
	Recovery	maximum of 2 test Restore requests per month. Excludes recovery testing which would be at an additional cost. Customer must purchase Backup Storage Service

See RACI chart in appendix I.5 ("RACI for Database Management") for more information about Database Management services and the roles of Customer and Virtustream.

B.3.5 Operating System Management

Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur when managing an operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description
OSM001	Storage and File Management	Create/delete/change file systems, build new virtual machines.
OSM002	User and Profile Management	Create/Delete/Change operating system users. profiles and policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, or via Capacity Management or Service Monitoring.
OSM005	Housekeeping	Create/delete/change vendor specific housekeeping best practices.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management services and the roles of Customer and Virtustream.

B.3.6 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Enterprise Database and Operating System Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM002	OS patches and hotfix	Implementation of supported OS patches (non-security), as well as hotfixes.	Monthly
PMM003	Critical Patches	Implementation of Critical and/or Security Patches.	Monthly

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

SCHEDULE C- SAP SUPPORT

C.1 Standard SAP Support

Overview for Standard SAP Support		
Section	**Service**	**Frequency**
C.1.1	**SAP Monitoring**	**24x7x365**
C.1.3	**Event Notification**	
II.1.1	**Responses to Incidents**	**Not included**
II.1.2	**Responses to Service Requests**	
	SAP Basis Management	

C.1.1 SAP Monitoring

Virtustream will provide "Monitoring Services", which include system monitoring and event monitoring. The system alerts Virtustream and selected Customer contacts highlighting areas that require attention or action. The Monitoring Services include the following:

Service Code	Service Name	Service Description	Frequency
SVM001	System Availability	Checks that SAP is available and accessible.	<1 minute
SVM009	Memory Management	Check SAP buffers.	Daily
SVM010	CPU Efficiency	Check CPU utilisation.	<1 minute
SVM022	File System Space	Check file system free space.	<1 minute

See RACI chart in appendix I.2 ("RACI for SAP Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

C.1.3 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

For Standard Support, alerts will be sent automatically, without Virtustream checking for false positives. Alerts will not automatically trigger the creation of a ticket in the service desk. Customer may create a ticket and request that Virtustream assist in resolving an issue. Customer will be charged at Virtustream's current time and material rates.

C.2 Business SAP Support

Overview for Business SAP Support		
Section	**Service**	**Frequency**
C.2.1	**SAP Monitoring**	**24x7x365**
C.2.2	**Operating System and Database Monitoring**	
C.2.3	**Event Notification**	
II.1.1	**Responses to Incidents**	**Monday-Friday, 8 AM EST- 5 PM EST.**
II.1.2	**Responses to Service Requests**	
C.2.4	**SAP Basis Management**	
C.2.5	**Database Management**	
C.2.6	**Operating System Management**	
C.2.7	**Patch Management**	**Monthly/As agreed to with Customer**

C.2.1 SAP Monitoring

Virtustream will provide "Monitoring Services", which include system monitoring and event monitoring. The system alerts Virtustream and selected Customer contacts highlighting areas that require attention or action. The Monitoring Services include the following:

Service Code	Service Name	Service Description	Frequency
SVM001	System Availability	Checks that SAP is available and accessible.	<1 minute
SVM002	Version Management	Details the current version levels in operation.	On Request
SVM003	Background Jobs	Check for failed background jobs. Based on Customer guidelines.	Automate via CCMS alerting
SVM005	IDOC Status	Check the status of the in-coming and out-going IDOC queues. Based on Customer guidelines	Queues will monitored continuously and can be reset if in a stuck status, errors or issues will need to be addressed by the clients middleware technical or functional team member
SVM006	RFC Communications	Check the status of the inbound and outbound communication queues. Based on Customer guidelines	Multiple times per day depending on which queue
SVM008	Response Times	Check the dialog response time.	Daily or upon request or as part of issue RCA
SVM009	Memory Management	Check SAP buffers.	Daily
SVM010	CPU Efficiency	Check CPU utilisation.	<1 minute
SVM011	System Security	Check that system has been locked against system modification and that as determined by the Customers predefined strategy is enforced.	<1 minute
SVM013	Update Failures	Check for failed updates.	Daily
SVM014	Lock Management	Check for long running lock enqueues.	<1 minute
SVM015	SAP Processes	Check for long running processes.	<1 minute
SVM016	Active Users	Monitor user activity in support of annual SAP license auditing.	On Request
SVM017	Program Failures	Check for ABAP failures.	Multiple times per day
SVM018	Backup	Checks that backups have been successfully completed. Check the timing/performance of backups.	Daily
SVM019	Output Management	Check for spool failures.	Daily or per ticket request
SVM020	SAP System Log	Check for critical or high warnings.	Daily
SVM022	File System Space	Check file system free space.	<1 minute

See RACI chart in appendix I.2 ("RACI for SAP Monitoring") for more information about Monitoring

Services and the roles of Customer and Virtustream.

C.2.2 Operating System and Database Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

C.2.3 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. A Major Alert will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST (for Business and Enterprise Support). A Critical Alert will be escalated 24x7x365 (for Enterprise Support).

The default Notification settings for Operating Systems are described in the table below:

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The most common default monitoring settings for databases are described in the table below:

Monitor	Notes	Default Threshold/Value	Alert
Database Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle	Running	Started	critical if stopped

Listener			
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any database resources.	This number should be "0" or "0" % wait time.	critical

C.2.4 SAP Basis Management

Virtustream will provide "Basis Management Services", which includes the day-to-day technical administration of the SAP systems as provided below. Business SAP support Includes 20 hours per month of Customer facing Basis Manager support. Additional time can be purchased if needed. The Basis Management Services include the following:

Service Code	Service Name	Service Description	Exclusions / limitations
BCM003	Transport & Correction Management	All transports are managed through Customer's change management process at pre-determined times as agreed to	Virtustream and Customer will mutually agree in advance as to the transport import schedule.
BCM004	Spool Management	Create/delete/change SAP printers.	
BCM005	Client Management	Creation of new empty clients. Deletion of clients. Client refresh within the same SAP instance.	
BCM006	CCMS Management	Create/delete/change operations timetable, operation modes, SAP load balancing groups, SAP instance profile, DBA planning schedule.	
BCM007	Background Job Management	Scheduling, release, cancellation and deletion of background jobs.	Virtustream and Customer will mutually agree in advance as to what actions to take as a result of

Service Code	Service Name	Service Description	Exclusions / limitations
			any deviations occurring, such as job interruptions, and such mutually agreed and Customer will supply the documented procedures accordingly.
BCM009	SAP Earlywatch	Review and implementation of appropriate SAP Basis Earlywatch recommendations.	In coordination with Customer's approval and predetermined change management process.
BCM010	Performance Management	Performance analysis, tuning, recording, maintenance and implementation of recommendations/solutions	This Service does not include improvement of the performance of Customer's ABAP / Java programs.
BCM012	SAP Restore and Recovery Advice	Advise on Restore/recovery of supported SAP systems.	
BCM013	SAP Refreshes	Perform instance refreshes of SAP supported SAP systems.	Max of 2 instance refreshes per quarter.

See RACI chart in appendix I.6 ("RACI for SAP Basis Management") for more information about SAP Basis Management services and the roles of Customer and Virtustream.

C.2.5 Database Management

Virtustream will provide "Database Management Services", which includes the day-to-day technical administration of the Database Systems. The Service will meet certain functions that occur when managing Relational Database Management Systems. The Database Management Services include the following:

Service Code	Service Name	Service Description
DBM001	Space Management	Manage all aspects of RDBMS space management for stability and availability of the RDBMS.
DBM002	Security Management	Implement security recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DBM003	Object Management	Manage all aspects of RDBMS object management for stability and availability of the system.
DBM004	Configuration Management	Implement configuration recommendations as required by the RDBMS vendor, SAP, Customer, or recommended via Service Monitoring.
DBM005	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.
DBM006	RDBMS Backup	Verify RDBMS backup tasks through RDBMS tools. Customer must purchase Backup Storage service
DBM007	RDBMS Restore and Recovery Advice	Advice on Restore/recovery of supported RDBMS. Customer must purchase Backup Storage service.

See RACI chart in appendix I.5 ("RACI for Database Management") for more information about Database Management services and the roles of Customer and Virtustream.

35

C.2.6 Operating System Management

Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur when managing an SAP operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description
OSM001	Storage and File Management	Create/delete/change file systems, create new virtual machines
OSM002	User and Profile Management	Create/Delete/Change operating system users. Profiles and policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, SAP, or via Capacity Management or Service Monitoring.
OSM004	Spooling and Printer Management	Create/delete/change printers, hold/remove spool requests.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management services and the roles of Customer and Virtustream.

C.2.7 SAP Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services include the following:

Service Code	Service Name	Service Description	Frequency
SYM001	SAP Kernel release	Implementation of SAP kernel release.	Quarterly upon request
SYM002	SAP Support Packages	Implementation of SAP support packages/content/ADDON/PLUGIN	
SYM003	RDBMS Maintenance release	Implementation of RDBMS maintenance release and service packs.	Quarterly upon request.
SYM004	RDBMS Patches / hotfix	Implementation of RDBMS patches and hotfixes.	Upon request.
SYM005	OS Patches	Implementation of OS patches.	Upon request

For more information, see appendix IV ("Patch Management")

C.3 Enterprise SAP Support

Overview for Enterprise SAP Support		
Section	Service	Frequency

C.3.1	SAP Monitoring	
C.3.2	Operating System and Database Monitoring	24x7x365
C.3.3	Event Notification	
II.1.1	Responses to Incidents	24x7x365
II.1.2	Responses to Service Requests	Monday-Friday, 8 AM EST- 5 PM EST.
C.3.4	SAP Basis Management	
C.3.5	Database Management	
C.3.6	Operating System Management	
C.3.7	SAP Patch Management	Monthly

C.3.1 SAP Monitoring

Virtustream shall provide the "Monitoring Services", which include system monitoring and event monitoring. The system alerts Virtustream and selected Customer contacts highlighting areas that require attention or action. The Monitoring Services include the following:

Service Code	Service Name	Service Description	Frequency
SVM001	System Availability	Checks that SAP is available and accessible.	<1 minute
SVM002	Version Management	Details the current version levels in operation.	On Request
SVM003	Background Jobs	Check for failed background jobs. Based on Customer guidelines.	Automate via CCMS alerting
SVM005	IDOC Status	Check the status of the in-coming and out-going IDOC queues. Based on Customer guidelines	Queues will monitored continuously and can be reset if in a stuck status, errors or issues will need to be addressed by the clients middleware technical or functional team member
SVM006	RFC Communications	Check the status of the inbound and outbound communication queues. Based on Customer guidelines	Multiple times per day depending on which queue
SVM008	Response Times	Check the dialog response time.	Daily or upon request or as part of issue RCA
SVM009	Memory Management	Check SAP buffers.	Daily
SVM010	CPU Efficiency	Check CPU utilisation.	<1 minute
SVM011	System Security	Check that system has been locked against system modification and that as determined by the Customers predefined strategy is enforced.	<1 minute
SVM013	Update Failures	Check for failed updates.	Daily
SVM014	Lock Management	Check for long running lock enqueues.	<1 minute
SVM015	SAP Processes	Check for long running processes.	<1 minute
SVM016	Active Users	Monitor user activity in support of annual SAP license auditing.	On Request

Service Code	Service Name	Service Description	Frequency
SVM017	Program Failures	Check for ABAP failures.	Multiple times per day
SVM018	Backup	Checks that backups have been successfully completed. Check the timing/performance of backups.	Daily
SVM019	Output Management	Check for spool failures.	Daily or per ticket request
SVM020	SAP System Log	Check for critical or high warnings.	Daily
SVM022	File System Space	Check file system free space.	<1 minute

See RACI chart in appendix I.2 ("RACI for SAP Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

C.3.2 Operating System and Database Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

C.3.3 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. A Major Alert will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST (for Business and Enterprise Support). A Critical Alert will be escalated 24x7x365 (for Enterprise Support).

The default Notification settings for Operating Systems are described in the table below:

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The most common default monitoring settings for databases are described in the table below:

Monitor	Notes	Default Threshold/Value	Alert
Database Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any database resources.	This number should be "0" or "0" % wait time.	critical

C.3.4 SAP Basis Management

Virtustream will provide "Basis Management Services", which includes the day-to-day technical

Service Code	Service Name	Service Description
CPM001	Capacity Report	Summarized report of a predefined period to aid in Capacity Management. Quarterly on request.

administration of the SAP systems as provided below. Enterprise SAP support Includes 20 hours per month of Basis Manager support. Additional time can be purchased if needed. The Basis Management Services include the following:

Service Code	Service Name	Service Description	Exclusions / limitations
BCM003	Transport & Correction	All transports are managed through Customer's change	Virtustream and Customer will mutually agree in advance as to

39

Service Code	Service Name	Service Description	Exclusions / limitations
	Management	management process at pre-determined times as agreed to	the transport import schedule.
BCM004	Spool Management	Create/delete/change SAP printers.	
BCM005	Client Management	Creation of new empty clients. Deletion of clients. Client refresh within the same SAP instance.	
BCM006	CCMS Management	Create/delete/change operations timetable, operation modes, SAP load balancing groups, SAP instance profile, DBA planning schedule.	
BCM007	Background Job Management	Scheduling, release, cancellation and deletion of background jobs.	Virtustream and Customer will mutually agree in advance as to what actions to take as a result of any deviations occurring, such as job interruptions, and such mutually agreed and Customer will supply the documented procedures accordingly.
BCM009	SAP Earlywatch	Review and implementation of appropriate SAP Basis Earlywatch recommendations.	In coordination with Customer's approval and predetermined change management process.
BCM010	Performance Management	Performance analysis, tuning, recording, maintenance and implementation of recommendations/solutions	This Service does not include improvement of the performance of Customer's ABAP / Java programs.
BCM012	SAP Restore and Recovery Advice	Advise on Restore/recovery of supported SAP systems.	
BCM013	SAP Refreshes	Perform instance refreshes of SAP supported SAP systems.	Max of 2 instance refreshes per quarter.

See RACI chart in appendix I.6 ("RACI for SAP Basis Management") for more information about SAP Basis Management services and the roles of Customer and Virtustream.

C.3.5 Database Management

Virtustream will provide "Database Management Services", which includes the day-to-day technical administration of the Database Systems. The Service will meet certain functions that occur when managing Relational Database Management Systems. The Database Management Services include the following:

Service Code	Service Name	Service Description
DBM001	Space Management	Manage all aspects of RDBMS space management for stability and availability of the RDBMS.
DBM002	Security	Implement security recommendations as required by the RDBMS

Service Code	Service Name	Service Description
	Management	vendor, Customer, or recommended via Service Monitoring.
DBM003	Object Management	Manage all aspects of RDBMS object management for stability and availability of the system.
DBM004	Configuration Management	Implement configuration recommendations as required by the RDBMS vendor, SAP, Customer, or recommended via Service Monitoring.
DBM005	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.
DBM006	RDBMS Backup	Verify RDBMS backup tasks through RDBMS tools. Customer must purchase Backup Storage service
DBM007	RDBMS Restore and Recovery Advice	Advice on Restore/recovery of supported RDBMS. Customer must purchase Backup Storage service.

See RACI chart in appendix I.5 ("RACI for Database Management") for more information about Database Management services and the roles of Customer and Virtustream.

C.3.6 Operating System Management

Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur when managing an SAP operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description
OSM001	Storage and File Management	Create/delete/change file systems, create new virtual machines
OSM002	User and Profile Management	Create/Delete/Change operating system users. Profiles and policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, SAP, or via Capacity Management or Service Monitoring.
OSM004	Spooling and Printer Management	Create/delete/change printers, hold/remove spool requests.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management services and the roles of Customer and Virtustream.

C.3.7 SAP Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes

applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services include the following:

Service Code	Service Name	Service Description	Frequency
SYM001	SAP Kernel release	Implementation of SAP kernel release.	Quarterly upon request
SYM002	SAP Support Packages	Implementation of SAP support packages/content/ADDON/PLUGIN	
SYM003	RDBMS Maintenance release	Implementation of RDBMS maintenance release and service packs.	Quarterly upon request*.*
SYM004	RDBMS Patches / hotfix	Implementation of RDBMS patches and hotfixes.	Upon request.
SYM005	OS Patches	Implementation of OS patches.	Upon request

For more information, see appendix IV ("Patch Management").

C.4 Additional Services

C.4.1 SAP BODS Administrator

An SAP BODS Administrator can be provided at an ad hoc hourly rate for specific services or as a service covering up to 12 instances per administrator. The SAP BODS Administrator services include the following:

Service Code	Service Name	Service Description	Exclusions / limitations
BCM001	Transport & Correction Management	All transports are managed through Customer's change management process at pre-determined times.	Virtustream and Customer will mutually agree in advance as to the transport import schedule.
BCM002	Spool Management	Create/delete/change SAP printers.	
BCM005	Background Job Management	Scheduling, release, cancellation and deletion of background jobs.	Virtustream and Customer will use good faith efforts to mutually agree in advance as to what actions to take as result of any deviations occurring such as job interruptions, and such mutually agreed and documented procedures will be followed.
BCM006	SAP Early watch	Review and implementation of appropriate SAP Basis EarlyWatch recommendations.	In coordination with Customer's approval and predetermined change management process.
BCM007	Performance Management	Performance analysis, tuning, recording, maintenance and implementation of recommendations/solutions.	This service does not include improvement of the performance of Customer's ABAP / Java programs.
BCM008	SAP Restore and Recovery Advice	Advise on restore/recovery of supported SAP systems.	
BCM010	System patches	System Patches based on customer or project requirements or issues.	This service doesn't include upgrades to the system. Upgrade will be T&M.

Service Code	Service Name	Service Description	Exclusions / limitations
BCM011	Repositories management	Creation of Repositories (local repositories, Central repository, QA repository, Production repository).	
BCM012	Job Servers	Creation of Job Servers as required by the customer or for the Project	
BCM013	Objects Migration	Migrating Jobs,Global variables,Substitution Parameters from one environment to other.	

SCHEDULE D- HANA SUPPORT

D.1 Standard HANA Support

Overview for Standard HANA Support		
Section	**Service**	**Frequency**
D.1.1	**Monitoring**	**24x7x365**
D.1.2	**Notification**	
II.1.1	**Responses to Incidents**	**Not included**
II.1.2	**Responses to Service Requests**	
	HANA Management	
	Operating System Management	
D.1.3	**Patch Management**	**Monthly**

D.1.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

D.1.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

For Standard Support, alerts will be sent automatically, without Virtustream checking for false positives. Alerts will not automatically trigger the creation of a ticket in the service desk. Customer may create a ticket and request that Virtustream assist in resolving an issue. Customer will be charged at Virtustream's current time and material rates.

The default Notification settings for Operating Systems are described in the table below:

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The most common default monitoring settings for HANA are described in the table below:

Monitor	Notes	Default Threshold/ Value	Alert
HANA Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any HANA resources.	This number should be "0" or "0" % wait time.	critical

D.1.3 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Standard HANA Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM003	Critical Patches	Implementation of Critical and/or Security Patches for supported **Microsoft** OS.	Monthly

With Standard Support, patches will be released to Customer's production environment without prior testing in Customer's QA environment.

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

D.2 Business HANA Support

Overview for Business HANA Support		
Section	**Service**	**Frequency**
D.2.1	**Monitoring**	**24x7x365**
D.2.2	**Notification**	
II.1.1	**Responses to Service Requests**	**Monday-Friday,**
II.1.2	**Responses to Incidents**	**8 AM EST- 5 PM EST.**
D.2.3	**HANA Management**	
D.2.4	**Operating System Management**	
D.2.5	**Patch Management**	**Monthly**

D.2.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

D.2.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. A Major Alert will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST (for Business and Enterprise Support). A Critical Alert will be escalated 24x7x365 (for Enterprise Support).

The default Notification settings for Operating Systems are described in the table below:

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The most common default monitoring settings for HANA are described in the table below:

Monitor	Notes	Default Threshold/Value	Alert
HANA Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any HANA resources.	This number should be "0" or "0" % wait time.	critical

D.2.3 HANA Management

Virtustream will provide "HANA Management Services", which includes the day-to-day technical administration of HANA Systems. The Service will meet certain functions that occur when managing HANA Systems. The HANA Management Services include the following:

Service Code	Service Name	Service Description
DMB001	Space Management	Manage all aspects of RDBMS space management for stability and availability of the RDBMS.
DMB002	Security Management	Implement security recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DMB003	Object Management	Manage all aspects of RDBMS object management for stability and availability of the system.
DMB004	Configuration Management	Implement configuration recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DMB005	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.
DMB006	RDBMS Backup	Initiate RDBMS backup tasks through RDBMS tools. Customer must purchase Backup Storage Service

Service Code	Service Name	Service Description
DMB007	RDBMS Restore and Recovery Advice	Advice on Restore/recovery of supported RDBMS. Customer must purchase Backup Storage Service. Combined maximum of 2 service requests per month
DMB008	RDBMS Recovery	Perform recovery of supported RDBMS Systems. A combined maximum of 2 test Restore requests per month. Excludes recovery testing which would be at an additional cost. Customer must purchase Backup Storage Service

See RACI chart in appendix I.5 ("RACI for Database Management") for more information about HANA Management services and the roles of Customer and Virtustream.

D.2.4 Operating System Management

Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur when managing an operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description
OSM001	Storage and File Management	Create/delete/change file systems, build new virtual machines.
OSM002	User and Profile Management	Create/Delete/Change operating system users. profiles and policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, or via Capacity Management or Service Monitoring.
OSM005	Housekeeping	Create/delete/change vendor specific housekeeping best practices.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management services and the roles of Customer and Virtustream.

D.2.5 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Business HANA Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM002	OS patches and hotfix	Implementation of supported OS patches (non-security), as well as hotfixes.	Upon request
PMM003	Critical Patches	Implementation of Critical and/or Security	Upon

Service Code	Service Name	Service Description	Frequency
		Patches.	request

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

D.3 Enterprise HANA Support

Overview for Enterprise HANA Support		
Section	**Service**	**Frequency**
D.3.1	**Monitoring**	**24x7x365**
D.3.2	**Notification**	
II.1.1	**Responses to Incidents**	**24x7x365**
II.1.2	**Responses to Service Requests**	**Monday-Friday, 8 AM EST- 5 PM EST.**
D.3.3	**HANA Management**	
D.3.4	**Operating System Management**	
D.3.5	**Patch Management**	**Monthly**

D.3.1 Monitoring

Virtustream will provide "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services include the activities set forth below:

Service Code	Service Name	Service Description	Frequency
AVM001	System Availability	Checks that Operating System is available.	<1 minute
AVM002	File System Space	Check that file system free space is available.	15 minutes
AVM003	Event Log Management	Monitor event logs for critical or error event levels.	<1 minute

See RACI chart in appendix I.3 ("RACI for Operating System and Database Monitoring") for more information about Monitoring Services and the roles of Customer and Virtustream.

D.3.2 Event Notification

Service Code	Service Name	Service Description
AVN001	Event Notification	Alerts for alarms thresholds being met or exceeded.

An alert will trigger the creation of a ticket in the Service Desk. A Major Alert will be escalated during normal business hours, Monday-Friday, 8 AM-5 PM EST (for Business and Enterprise Support). A Critical Alert will be escalated 24x7x365 (for Enterprise Support).

The default Notification settings for Operating Systems are described in the table below:

Metric Name	Alert Critical	Alert – Major	Samples X Frequency
QOS_CPU_USAGE	99 %	98 %	12 X 5 mins
QOS_DISK_USAGE_PERC	< 2%	< 5%	4 X 15 mins
QOS_MEMORY_PAGING	99%	98%	12 X 5 mins
QOS_MEMORY_PERC_USAGE	30000 KB/Sec	25000 KB/Sec	12 X 5 mins
QOS_MEMORY_PHYSICAL_PERC	99%	98%	12 X 5 mins
QOS_MEMORY_SWAP_PERC	99%	98%	12 X 5 mins
Server Reboot	True		Alert based on system log
Disk Missing	True		12 X 5 mins

The most common default monitoring settings for HANA are described in the table below:

Monitor	Notes	Default Threshold/Value	Alert
HANA Availability			
Tablespace Free	Percentage of free space on each tablespace.	80%	major
Log File Size (SQL)	Less than 1 GB Available	<1 GB	critical
SQL Agent/Oracle Listener	Running	Started	critical if stopped
Cache-Hit Ratio	The buffer cache hit ratio calculates how often a requested block has been found in the buffer cache without requiring disk access.	95%	major
User Memory Consumption		80%	major
Concurrent Users	Number of users on at any given time.	200	major
Memory Usage	Total memory used before usage causes issues with db performance.	90%	critical
Session Waits counter	Set is how many users are waiting for resources. Recommendation is to use the 0% wait, meaning no process should have to wait for any HANA resources.	This number should be "0" or "0" % wait time.	critical

D.3.3 HANA Management

Virtustream will provide "HANA Management Services", which includes the day-to-day technical administration of the HANA Systems. The Service will meet certain functions that occur when managing Relational HANA Management Systems. The HANA Management Services include the following:

Service Code	Service Name	Service Description
DMB001	Space Management	Manage all aspects of RDBMS space management for stability and availability of the RDBMS.
DMB002	Security Management	Implement security recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.
DMB003	Object Management	Manage all aspects of RDBMS object management for stability and availability of the system.
DMB004	Configuration Management	Implement configuration recommendations as required by the RDBMS vendor, Customer, or recommended via Service Monitoring.

Service Code	Service Name	Service Description
DMB005	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.
DMB006	RDBMS Backup	Initiate RDBMS backup tasks through RDBMS tools. Customer must purchase Backup Storage Service
DMB007	RDBMS Restore and Recovery Advice	Advice on Restore/recovery of supported RDBMS. Customer must purchase Backup Storage Service. Combined maximum of 2 service requests per month
DMB008	RDBMS Recovery	Perform recovery of supported RDBMS Systems. A combined maximum of 2 test Restore requests per month. Excludes recovery testing which would be at an additional cost. Customer must purchase Backup Storage Service

See RACI chart in appendix I.5 ("RACI for Database Management") for more information about HANA Management services and the roles of Customer and Virtustream.

D.3.4 Operating System Management

Virtustream will provide "Operating System Management Services", which include the day-to-day technical management of the operating system. The Services will meet certain functions that occur when managing an operating system. The Operating System Management Services include the following:

Service Code	Service Name	Service Description
OSM001	Storage and File Management	Create/delete/change file systems, build new virtual machines.
OSM002	User and Profile Management	Create/Delete/Change operating system users. profiles and policies as well as group management are excluded
OSM003	Configuration Management	Create/delete/change operating system parameters to the configuration files as recommend by the OS vendor, or via Capacity Management or Service Monitoring.
OSM005	Housekeeping	Create/delete/change vendor specific housekeeping best practices.
OSM006	Operations Management	Stop and start of the operating system, system services and processes.
OSM007	Scheduling	Create/Delete/Change background scheduling services.
OSM008	Performance Management	Performance analysis, tuning, maintenance and implementation of recommendations/solutions.

See RACI chart in appendix I.4 ("RACI for Operating System Management") for more information about Operating System Management services and the roles of Customer and Virtustream.

D.3.5 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch Management Services for Enterprise HANA Support include the following:

Service Code	Service Name	Service Description	Frequency
PMM002	OS patches and hotfix	Implementation of supported OS patches (non-security), as well as hotfixes.	Upon request
PMM003	Critical Patches	Implementation of Critical and/or Security Patches.	Upon Request

For more details, including patch release schedule and QA environment testing, see appendix IV ("Patch Management") and RACI chart in appendix I.7 ("RACI for Patch Management").

SCHEDULE E- EXTRA SERVICES

Virtustream can provide services outside of the scope of Standard, Business and Enterprise support levels. Customer will contact the Service Desk (see appendix II "CCS Service Desk") to request one or more of the extra services detailed in this Schedule E ("Extra Services") according to the Service Request Process (appendix II.5 "Service Request Process"). Additional costs will apply to these services, which will be billed at Virtustream's current time and materials rates.

Standard Support customers can also request services listed under Business and Enterprise support, and incident management, at additional cost.

See also section 6 ("Technical Account Management Services (TAMS)") for account management services outside the scope of Standard, Business, and Enterprise support.

E.1 Professional Services
Professional services can be purchased ad hoc. the roles available to be purchased are as follows:

CPT SKU	Role
CC-LAB-ONPG-MAN	Onshore Program Manager
CC-LAB-ONPJ-MAN	Onshore Project Manager
CC-LAB-ONMC-CON	Onshore Certified Migration Consultant
CC-LAB-ONOB-MAN	Onshore Onboarding Manager
CC-LAB-ONOB-SRC	Onshore Onboarding Senior Consultant
CC-LAB-ONOB-CON	Onshore Onboarding Consultant
CC-LAB-ONBH-MAN	Onshore Basis / HANA Manager
CC-LAB-ONBH-SRC	Onshore Basis / HANA Senior Consultant
CC-LAB-ONBH-CON	Onshore Basis / HANA Consultant
CC-LAB-ONSB-MAN	Onshore SAP Basis Manager
CC-LAB-ONSB-SRC	Onshore SAP Basis Senior Consultant
CC-LAB-ONSB-CON	Onshore SAP Basis Consultant
CC-LAB-ONSF-MAN	Onshore SAP Functional Manager
CC-LAB-ONSF-SRC	Onshore SAP Functional Senior Consultant
CC-LAB-ONSF-CON	Onshore SAP Functional Consultant
CC-LAB-ONOD-MAN	Onshore OS/DB Manager
CC-LAB-ONOD-SRC	Onshore OS/DB Senior Consultant
CC-LAB-ONOD-CON	Onshore OS/DB Consultant
CC-LAB-ONNT-MAN	Onshore Network Manager
CC-LAB-ONNT-SRC	Onshore Network Senior Consultant
CC-LAB-ONNT-CON	Onshore Network Consultant
CC-LAB-ONBR-MAN	Onshore Backup and Recovery Manager
CC-LAB-ONBR-SRC	Onshore Backup and Recovery Senior Consultant
CC-LAB-ONBR-CON	Onshore Backup and Recovery Consultant
CC-LAB-OFOD-CON	Offshore OS/DB Consultant
CC-LAB-OFBO-ADM	Offshore SAP BODS Administrator
CC-LAB-OFSB-MAN	Offshore SAP Basis Manager
CC-LAB-OFBH-CON	Offshore SAP Basis Senior Consultant

CC-LAB-OFBS-CON	Offshore SAP Basis Consultant
CC-LAB-OFBW-LD	Offshore BW Senior Lead
CC-LAB-OFBW-CON	Offshore BW Consultant
CC-LAB-OFSS-ENG	Offshore Security Services Engineer
CC-LAB-OFBO-CON	Offshore BO Designer Consultant

E.2 Operating System and Database Monitoring

Virtustream can provide additional "Monitoring Services", which include observing events in near real-time. Virtustream support teams will monitor event behavior in such a way that they can be proactive, identifying problems and potential event outages before they occur.

Supported Systems (see appendix III) will be monitored using xStream monitoring, 24x7x365. Monitoring Services that are not included with any support offer but can be requested at an additional cost include the activities set forth below:

Service Code	Service Name	Service Description
AVM004	System Usage/Utilization	Monitor system performance counters such as CPU and Memory utilization, disk I/O, and network I/O. Disk I/0 and Network I/O custom report requested via TAM
AVM005	Service/Daemon/ Process State	Monitor the state of system services (Windows), daemons (Linux), and processes

E.3 SAP Monitoring

Virtustream can provide additional "Monitoring Services", which include system monitoring and event monitoring. The system alerts Virtustream and selected Customer contacts highlighting areas that require attention or action. The Monitoring Services that are not included with any support offer but can be requested at an additional cost include the following:

Service Code	Service Name	Service Description
SVM007	Workflow	Check workflow failures.
SVM012	User Security	Check for failed logon attempts.

E.4 SAP Basis Management

Virtustream can provide additional "Basis Management Services", which includes the day-to-day technical administration of the SAP systems as provided below. The Basis Management Services that are not included with any support offer but can be requested at an additional cost include the following:

Service Code	Service Name	Service Description
BCM014	SAP Data Management	Create/delete/change/fix SAP Master Data, SAP Transactional Data and SAP Configuration Data.

E.5 Patch Management

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware, or to improve the functionality of software or hardware. Virtustream can provide extra "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work. The Patch

54

Management Services that are not included with any support offer but can be requested at an additional cost include the following:

E.5.1 Operating System and Database Patch Management

Service Code	Service Name	Service Description
PMM001	Service Packs	Implementation of OS and RDBMS service packs.
PMM004	Major Release Upgrades	Major release of OS and RDBMS software

E.5.2 SAP Patch Management

Service Code	Service Name	Service Description
SYM006	Major Release Upgrades	Major release of RDBMS or SAP software, including support package stacks and enhancement packs

APPENDIX I- RASCI CHARTS

I.1 Definitions for RASCI charts:

Responsible: the party responsible for ensuring that the task, function, or deliverable described is completed accurately and timely; often known as the "doer".

Accountable: the party to whom "R" is accountable and is the authority who approves or signs off on work before it is effective.

Supportive: the party who provides resources or plays a supporting role to the extent reasonably necessary to complete the task, function, or deliverable. When Virtustream is "Supportive", Virtustream may charge Customer on a time and materials basis for its resources used to "Support"

Consulted: the party who reviews output or progress necessary to complete the task, function, or deliverable. When Virtustream is "Consulted" by Customer, Virtustream may charge Customer on a time and materials basis for its resources used to provide such consulting.

Informed: the party who needs to be notified of results, completion, or deliverable but need not necessarily be consulted.

I.2 RACI for SAP Monitoring

Service Code	Service Name	Service Description	Virtustream	Customer
AVM001	system availability	Checks that OS, RDBMS or applications are available.	RA	CI
AVM002	file system space	Check file system free space is available	RA	CI
AVM003	event log management	Monitor Event Logs for critical or error event levels	RA	CI
AVM004	system usage/utilization	Monitor CPU, Memory and other system counters that measure usage or utilization	RA	CI
AVM005	Service/Daemon/Process State	Monitor the up down, stopped or start of specific services/daemons and named processes	RA	CI

I.3 RACI for Operating System and Database Monitoring

Service Code	Service Name	Service Description	Virtustream	Customer
AVM001	system availability	Checks that OS, RDBMS or applications are available.	RA	CI
AVM002	file system space	Check file system free space is available	RA	CI

			Virtustream	Customer
AVM003	event log management	Monitor Event Logs for critical or error event levels	RA	CI
AVM004	system usage/utilization	Monitor CPU, Memory and other system counters that measure usage or utilization	RA	CI
AVM005	Service/Daemon/ Process State	Monitor the up down, stopped or start of specific services/daemons and named processes	RA	CI

I.4 RACI for Operating System Management

Service Name	Service Description	Virtustream	Customer
OSM001: Storage And File Management	Add new disk or file system to a virtual machine	RA	CI
	Delete a disk or file system form a virtual machine	RA	CI
	Extend disk or file system on a virtual machine	RA	CI
	Shrink disk or file system on a virtual machine	RA	CI
	Build new virtual machines	RA	CI
OSM002: User And Profile Management	Create new local user account with Customer approval	RA	CI
	Delete new local user account with Customer approval	RA	CI
	Modify new local user account with Customer approval	RA	CI
OSM003: Configuration Management	Add OS level parameters to improve system performance based on vendor specific recommendations or information gathered from Capacity Management or Service Monitoring	RA	CI
	Delete OS level parameters to improve system performance based on vendor specific recommendations or information gathered from Capacity Management or Service Monitoring	RA	CI
	Modify OS level parameters to improve system performance based on vendor specific recommendations or information gathered from Capacity Management or Service Monitoring	RA	CI
	Application install and configuration (e.g., I.E. IIS, Apache)	CI	RA
OSM004: Spooling And Printer Management (Applies Only When Sap Services Are Purchased)	Delete print jobs/spool on request	RA	CI
	Add new printers for inoperability with SAP	RA	CI
	Remove printers from the SAP system as requested	RA	CI
	Modify printers for inoperability with SAP	RA	CI
	Provide the proper SAP print reorganization and maintenance jobs are run according to SAP best practice	RA	CI
OSM006: House Keeping	Add OS level parameters for compliance with OS vendor best practices	RA	CI
	Delete OS level parameters for compliance with OS	RA	CI

57

	vendor best practices		
	Modify OS level parameters for compliance with OS vendor best practices	RA	CI
	RDBMS vendor relationship, Customer provided	I	RAC
	RDBMS vendor relationship, Virtustream provided	RAC	I
OSM007: Operations Management	Stop and start of the operating system, system services and processes	RA	CI
OSM008: Scheduling	Setup scheduled jobs as requested	RA	CI
	Delete scheduled jobs as requested	RA	CI
	Modify scheduled jobs as requested	RA	CI
OSM008: Scheduling (applies only when SAP services are purchased)	Setup batch jobs as requested by users	RA	CI
	Reschedule, pause or delete predefined batch jobs on request	RA	CI
	Report failed batch jobs	RA	CI
	Maintain Basis related system batch jobs	RA	CI
OSM009: Performance Management	Performance analysis, tuning, maintenance and implementation of recommended solutions	RA	CI

I.5 RACI for Database Management

		SAP		NON SAP		
DB #	Role/Function	Virtustream	Customer	Virtustream	Customer	Service Code
1.0	**System level Database Management - SQL/Oracle**					
1.1	Installing new database versions	R/A	C	R/A (at Customer's option)	R/A (at Customer's option)	DBM004
1.2	Applying publically available maintenance fixes supplied by the database vendor	R/A	C	R/A	C	PMM002
1.3	Setting and tuning system parameters	R/A	C	R/A	C	DBM004
1.4	Ensuring proper storage is available for databases	R/A	C	R/A	C	DBM001
1.5	System level Strategy Determination	R/A	C	R/A	C	DBM004
1.6	System Level planning and management	R/A	C	R/A	C	DBM004
1.7	System level implementations or installations	R/A	C	R/A	C	DBM004
1.8	Recommendation for System level tuning of the database parameters	R/A	C	R/A	C	DBM005

1.9	System level database monitoring and management	R/A	C	R/A	C	AVM001
1.10	System Level database recovery activities	R/A	C	R/A	C	DBM007
1.11	Perform Database System storage Capacity Management and provide estimates for the storage necessary to support the Database Systems	R/A	C	R/A	C	DBM001
1.12	Implement and administer system level components of the data archiving processes for the Database Systems	R/A	C	R/A	C	
1.13	Establish, manage and maintain authentication IDs and privileges	R/A	R/A	C	R/A	DBM002
1.14	Provide role-based access to Authorized Users to the Database Systems	C	R/A	C	R/A	DBM002
1.15	Develop security and access profiles and procedures for Database System administrators	R/A	R/A	C	R/A	DBM002
1.16	Develop and maintain scripts, utility jobs and automated processes necessary to maintain the Database Systems	R/A	C	R/A	C	DBM004
1.17	Alert log monitoring	R/A	C	R/A	C	AVM003
1.18	Trace files / logs cleanup	R/A	C	R/A	C	DBM006
1.19	Alert log file rotation	R/A	C	R/A	C	DBM006
1.20	Database backup monitoring (full/incremental/archive)	R/A	C	R/A	C	AVM003
1.21	Create Tablespace usage report	R/A	C	R/A	C	DBM005
1.22	Create Invalid Objects report	R/A	C	R/A	C	DBM005
1.23	Create New Object Creation Report	R/A	C	R/A	C	DBM005
1.24	Create Fragmented Object Report	R/A	C	R/A	C	DBM005
1.25	Create report on database usage statistics	R/A	C	R/A	C	DBM005
1.26	Create new DB instance	R/A	C	C	R/A	DBM003
1.27	Manage online redo logs or archive logs	R/A	C	R/A	C	DBM006
1.28	Stop & Start Services (Automate)	R/A	C	R/A	C	DBM005
2.0	**Backup/Restore**					
2.1	Develop, test, and implement logical backup/recovery strategy	C	R/A	C	R/A	

2.2	Develop, test, and implement System Level backup/recovery strategy	R/A	C	R/A	C	DBM006
2.3	System Level backup/Restore monitoring	R/A	C	R/A	C	AVM001, DBM006
2.4	Logical backup/Restore monitoring	R/A	R/A	R/A	R/A	AVM001, DBM006
2.5	Produce System level backup/Restore implementation and operational procedures	R/A	C	R/A	C	DBM006
2.6	Produce logical backup/Restore implementation and operational procedures	C	R/A	C	R/A	
3.0	**Database Monitoring Tasks (Events Monitored)**					
3.1	Connect check	R/A	C	R/A	C	AVM001
3.2	Connect DB	R/A	C	R/A	C	AVM001
3.3	Listener status	R/A	C	R/A	C	AVM001
3.4	Instance status	R/A	C	R/A	C	AVM001
3.5	RAC member status	R/A	C	R/A	C	AVM001
3.6	Datafile cannot extend	R/A	C	R/A	C	AVM001
3.7	Free space in Tablespace	R/A	C	R/A	C	AVM001
3.8	Free space deficit	R/A	C	R/A	C	AVM001
3.9	DBA - locks	R/A	C	R/A	C	AVM001
3.10	License limit	R/A	C	R/A	C	
3.11	Process limit	R/A	C	R/A	C	AVM001
3.12	ASM DG group	R/A	C	R/A	C	AVM001
3.13	Performance management & performance trends	R/A	C	R/A	C	AVM001
4.0	**Logical/Application DBA**					
4.1	Database design for a specific application	C	R/A	C	R/A	Customer staff to support these functions
4.2	Writing and debugging SQL code	C	R/A	C	R/A	
4.3	Logical strategy determination	C	R/A	C	R/A	
4.4	Logical planning and management	C	R/A	C	R/A	
4.5	Logical implementation or installations	C	R/A	C	R/A	
4.6	Recommendation of logical tuning database parameters	C	R/A	C	R/A	
4.7	Logical database monitoring and management	C	R/A	C	R/A	

60

4.8	Develop and maintain scripts, utility jobs and automated processes necessary to maintain the logical databases	R/A	R	C	R/A
4.9	Implement and administer logical components of the **data** archiving processes for the Database Systems	C	R	C	R/A
4.10	Logical database recovery activities	C	R	C	R
4.11	Manage and track database administration authentication IDs and privileges assigned to DBA team members for auditing compliance	R/A	R/A	I	R/A
4.12	Establish and maintain security and access procedures for Database System administrators to meet audit requirements	R/A	R/A	I	R/A

I.6 RACI for SAP Basis Management

Tasks	Virtustream	Customer	Comment
System Management			
SAP transport	R,A	I	
Resolution of Incident/Service tickets	R,A	R	
Printer definition	R,A	R	
Printer and output troubleshooting	R,A	C	
OSS note application	R,A	C	
OSS connection management	R,A	C	
Management and implementation of enhancement packs	R,A	R	Provided at Virtustream's time and materials rates
Nimsoft alert definitions	R,A	C	
Nimsoft alert setup	R,A	C	
Monitor system logs for errors and warnings.	R,A		
Monitor user activity and work process status.	R,A		
Monitor background jobs.	R,A	I	
Troubleshoot and resolve system background job issues.	R,A		
Troubleshoot and resolve functional/business application background job issues.	C	R,A	
Monitor lock entries.	R,A		
Monitor abnormal program failures.	R,A	C	
Monitor update failures.	R,A	C	
Monitor Transport Management System.	R,A		
Monitor communication channels (RFCs, ICM, Message Server, etc.)	R,A		
Troubleshoot and resolve system issues.	R,A	I	
Monitor and tune system performance.	R,A	C	

61

	Virtustream	Customer	
Monitor for performance issues and bottlenecks in application code.	R,A	I	
Perform application code tuning.	C	R,A	
Batch job monitoring and management (per documented process)	R,A	R,C	
Interface scheduling and monitoring (per documented process)	R,A	R,C	
Manage short dumps	R,A	C,I	
System log file analysis/management/resolution	R,A	C,I	
Application administration & troubleshooting	R,A	C,I	
Application patches update	R,A	C	
SAP client maintenance	R,A	C,I	
Shift handover / KT of new VS resource	R,A	C,I	
Planning of SAP system/landscape	R,A	R,A	
Perform application startup and shutdown.	R	A	
Operating System Administration			
Monitor CPU and memory utilization.	R,A	I	
Monitor file system usage.	R,A	I	
OS patches update	R,A	C,I	
Troubleshoot and resolve operating system issues.	R,A	I	
Output Management			
Monitor spool system for errors.	R,A	I	
Troubleshoot and resolve system printing issues.	R,A	I	
Troubleshoot and resolve site printing issues.	C	R,A	
Setup and test system printers.	R,A	C	
Setup and test site printers.	C	R,A	
Client and Change Management			
Perform client and system copies.	R	A	
Manage transport management system configuration.	R	A	
Apply transports and migrate configuration and code changes.	R	A	
Software Management			
Document software versions and end of support dates.	R,A	I	
Apply SAP software updates (e.g., support packages, kernel, etc.)	R	A	As requested quarterly
Apply database software updates (e.g., service packages, etc.)	R	A	
Apply OS software patches and updates	R	A	
Install new applications and software components.	R	A	Performed pursuant to a new SOW agreed to by the parties

I.7 RACI for Patch Management

Role/Function	Virtustream	Customer	Service Code
Automated Patching/scheduling (OS)	R,A	I,C	PMM001
Patch notification (OS)	R,A	I,C	PMM001
Patch staging - non-critical (OS)	R,A	I,C	PMM002

I.8 RASCI for Incident Management

Role/Function	Virtustream	Customer

62

Document, track and manage all Incidents using ITSM system (ITIL methodology/practices)	R/A	S
Perform Incident management related services necessary to meet Service Levels	R/A	S
Assign Incident priority based on impact and standards set forth above	R/A	S
Provide method of collaboration to address high priority Incidents (e.g. P1 bridge)	R/A	S
Communicate to Customer on the progress made to resolve Incidents and applicable work-arounds	R/A	S
Provide recommendations to avoid the reoccurrence of Incidents, develop and update knowledge base articles	R/A	S

I.9 RACI for Service Requests

Role/Function	Virtustream	Customer
Service Request Fulfillment		
Document, track and manage all Service Requests using ITSM system	R/A	S
Manage Service Requests to meet Service Levels	R/A	I
Obtain Virtustream internal approvals as needed	R/A	I
Obtain approvals from Customer based on possible impact from a requested change based on Virtustream's risk assessment	R/A	S
Notify Customer if unable to fulfill Service Request to meet Service Levels	R/A	I

I.10 RASCI for Problem Management

Role/Function	Virtustream	Customer
Request Root Cause Analysis tickets by contacting the Virtustream TAM (Customer requests Incident report/Problem record)	S	R/A
Document, track and manage all Problem tickets using ITSM system	R/A	S
Provide Problem management review and Root Cause Analysis (RCA) for all in-scope P 1 Incidents (preliminary report within 48 hours; final within 15 calendar days)	R/A	S
Provide Problem management and RCA of identified Problems (e.g., reoccurring events, alerts) - investigate and diagnose	R/A	S

APPENDIX II- CCS SERVICE DESK

Virtustream Service Desk Contact Details	
Hours of Support	24 x 7 x 365
Contact Number	1-877-303-9524
Email Address	XOC@virtustream.com
Service Management Portal	https://dashboard.vitustream.com
Language	English

II.1 Overview

The Virtustream Service Desk will perform the primary functions of Responding to Service Requests and Incidents. Primary contact shall be via email. Toll-free telephone support and a Service Management Dashboard which provides access to a ticketing self-service portal shall also be made available. Only representatives nominated during the onboarding process or through a service request will be able to report Incidents or Request Services via the Service Desk.

All tickets logged via email are considered a Service Request unless Customer informs the service desk that the problem is an Incident.

II.1.1 Incidents

Virtustream's Service Desk will respond to Incidents reported by Virtustream's Monitoring software or by Customer in the manner set forth in appendix II.4 ("Incident Reporting Process"), notify the Customer if Virtustream becomes aware of the Incident prior to Notification from Customer, and develop a Resolution Plan (see appendix II.4.1 "Resolution Plan").

See RACI chart in appendix I.8 ("RACI for Incident Management") for more information about the roles of Customer and Virtustream.

II.1.2 Service Requests

Virtustream's Service Desk will respond to Service Requests from Customer and resolve the request in the manner set forth in appendix II.5 ("Service Request Process"). All service requests must be submitted via a service desk request.

II.2 Support Levels

Nominated representatives can always contact the service desk, regardless of support level. Monitoring and Notification is always included 24x7x356. Responses to Incidents and Service Requests requires Business or Enterprise Support, and will be carried out during the times listed below:

Service	Standard	Business	Enterprise
Monitoring	24x7x365	24x7x365	24x7x365
Notification			
Responses to Service Requests	Not included	Monday-Friday, 8 AM EST-5 PM EST	Monday-Friday, 8 AM EST-6 PM EST

Responses to Incidents			24x7x365
Notes	Virtustream can provide access to an engineer at a T&M basis during normal business hours, Monday-Friday, 8 AM EST-5 PM EST.	After hours support is not included and hourly support rates will apply. Overnight support requires a ticket, along with escalation from an authorized user by phone to the Service Desk. Any emails or XOC tickets sent after normal business hours without a call to the Service Desk for escalation by an authorized user will be handled on the next business day.	Full support, and overnight monitoring and emergency support as needed. Overnight support requires a ticket, along with escalation from an authorized representative by phone to the Service Desk. Any emails or XOC tickets sent after normal business hours without a call to the Service Desk for escalation by an authorized user will be handled on the next business day.

II.3 Service Management Dashboard (Self-Service Portal)

Virtustream shall provide a Service Management Dashboard which provides access to a self-service portal, accessible with Virtustream-provided credentials. The Service Management Dashboard shall provide access to applets that allow Customer to create and update service management requests and to report Incidents. The dashboard shall also provide access to a standardized display for some of the foundational infrastructure monitoring, if those Services have been purchased by Customer. Customer dashboards are available via professional services engagement. Dashboard user credentials can be requested via the Virtustream Service Desk by Customer's nominated representatives to the Virtustream Service Desk.

II.4 Incident Reporting Process

To report an Incident, one of Customer's nominated representatives will contact the Virtustream Service Desk via telephone, email, or via the Service Management Portal using the contact details set forth above ("Virtustream Service Desk Contact Details"). Where initial contact is via telephone, the Customer will provide additional details via email to the email address above. In the event Virtustream becomes aware of the Incident prior to Notification from Customer, Virtustream shall provide email notification to Customer of the occurrence of the Incident. Following the Response, Virtustream will conduct an initial analysis, and prepare a resolution plan and outline the steps needed to resolve the issue, and an estimated fault resolution time.

II.4.1 Resolution Plan

Virtustream will develop a resolution plan which will be communicated to Customer via the Virtustream Service Desk.

II.5 Service Request Process

Service Requests shall be submitted by one of Customer's nominated representatives to the Virtustream Service Desk.

Virtustream shall provide a Response to such Service Request received from, or approved by, nominated representatives with the within sixty (60) minutes. Virtustream shall within one (1) business day of such request inform Customer of the anticipated completion date and time of such Service Request. Time frames will vary based on nature of the Service Request. Unless otherwise agreed by the parties, Service Requests are not reviewed outside of normal business hours (Monday-Friday, 8AM-5PM ET), without prior written agreement of Virtustream.

II.6 Incident & Service Request Prioritization

II.6.1 Escalations within Virtustream

Virtustream will provide Level 0 and Level I support and first call resolution where possible, as determined by Virtustream. Where first call resolution is not possible, the Virtustream Service Desk provides incident management for Incidents and Urgent Service Requests escalated to Level II and Level III resources as defined below.

In the event that Virtustream's Response to an Incident is not acceptable to the Customer, Customer can contact the Virtustream Service Desk and request escalation to the head of the Service Desk. Virtustream shall, upon receipt of any such request, immediately escalate the issue to the head of the Service Desk or technical team as appropriate.

II.6.2 Service Request Prioritization

Service Requests are assigned a priority of either 'Urgent' or 'Standard' and are queued for fulfillment with the corresponding priority. All Service Requests will be reviewed by the Virtustream Service Desk, who will determine the appropriate priority to assign with collaboration of Customer.

II.6.3 Incident Prioritization

All Incidents that are reported to the Virtustream Service Desk, or that Virtustream otherwise becomes aware of, will be initially assigned a priority by the Virtustream Service Desk as set forth below. Internal escalation for Incidents to Level II and Level III resources are based on the priority level assigned to the Incident.

Incident Prioritization		
Priority/Severity	**Definition**	**Response Time Service Level**
1	Major part of the system is unavailable/not operating correctly, affecting multiple users. No workarounds in place and business operations are not possible. **Or** Incident has a critical impact on the business (e.g., loss of the Exchange Production server impacting all users).	**30 minutes**	Response time will be within indicated time beginning from when the customer

2	Part of the system is unavailable/not operating correctly, affecting users in a single function. No workarounds in place and business operations in this function are not possible/severely impacted. **Or** Incident has a serious impact on part of the business (e.g., a configuration change is impacting a small subset of users).	**60 minutes**	creates a ticket or a monitoring event is validated. Additional resources are engaged via Virtustream's on Call Process.
3	Part of the system is unavailable/not operating correctly, affecting users in a single function. Workarounds in place, but business operations are impacted, although not severely. **Or** Incident has a temporary impact on users and is non critical or is a development issue (e.g., email is slow to deliver)	**4 hours**	
4	Incident that is causing inconvenience to the business, but not impacting operations. **Or** Incident has a minor impact on users or business, or issue is a request for further information	**1 business day**	

II.7 Problem Management
In the event that a Customer is experiencing a Problem, the Customer may request a Root Cause Analysis (RCA) ticket by contacting the Virtustream TAM. Virtustream will produce a preliminary RCA for all in-scope P1 Incidents within 48 hours, and a final report within 15 calendar days. Virtustream will Investigate and diagnose the Problem with the support of Customer and the RCA.

See RACI chart in appendix I.10 ("RACI for Problem Management") for more information about the roles of Customer and Virtustream.

APPENDIX III- SUPPORTED SYSTEMS

Virtustream will provide support for the Operating Systems and Relational Database Management Systems listed below, in the manner set forth in schedule A ("Operating System Support") and Schedule B ("Database Support").

III.1   Operating Systems
The following Operating Systems are supported by Virtustream:

Operating Systems		
OS	**Version**	**Comments**
Windows	Reference Windows Support Lifecycle End of extended support http://support.microsoft.com/gp/lifeselectindex	Support is reduced to best effort for OS versions that are no longer supported by vendor.
RedHat	Supported through End of Production Phase https://access.redhat.com/site/support/policy/updates/errata/	Patch management for RedHat and Centos is only available for Business and Enterprise support.
Centos	Supported through End of Life http://wiki.centos.org/Download	

III.2   Relational Database Management Systems
The Following Relational Database Management Systems are supported by Virtustream:

RDBMS		
Database	**Version**	**Comments**
MS SQL	Reference Windows Support Lifecycle End of extended support http://support.microsoft.com/gp/lifeselectindex	Support is reduced to best effort for Database versions that are no longer supported by vendor
Oracle	Support through Extended support defined: http://www.oracle.com/us/support/library/lifetime-support-technology-069183.pdf	

APPENDIX IV- PATCH MANAGEMENT

To maintain stability and performance, vendors regularly provide release updates and bug fixes to correct software or hardware. Virtustream will provide "Patch Management Services", which includes applying these updates and carrying out offline maintenance where the system must be taken down to carry out the work.

9.1 Operating System and Database Patch Management

Patch Management for Standard Operating System and Database (including HANA) Support only includes Critical Patches (PMM003) for supported Microsoft Operating Systems only (see Appendix III "Supported Systems"). Patch management for Databases only includes Critical Patches.). Patching will only be provided for RHEL and SUSE Operating Systems with licences provided by Virtustream. Service Packs and Major Release Upgrades for Operating Systems and Databases can be requested at an additional cost (see Schedule E "Extra Services").

Service Code	Service Name	Service Description	Frequency
PMM002	OS patches and hotfix	Implementation of supported OS patches (non-security), as well as hotfixes.	Monthly
PMM003	Critical Patches	Implementation of Critical and/or Security Patches.	Monthly

For more details, see RACI chart in appendix I.7 ("RACI for Patch Management").

9.2 SAP Patch Management

Patch Management for Standard SAP support only includes Critical Patches for supported Microsoft Operating Systems only (see Appendix III "Supported Systems"). SAP Patch Management includes Operating System and Database Patch Management. Major release upgrades, including support package stacks and enhancement packs, can be requested at an additional cost (see Schedule E "Extra Services").

Service Code	Service Name	Service Description	Frequency
SYM001	SAP Kernel release	Implementation of SAP kernel release.	Quarterly basis
SYM002	SAP Support Packages	Implementation of SAP support packages/content/ADDON/PLUGIN	
SYM003	RDBMS Maintenance release	Implementation of RDBMS maintenance release and service packs.	Quarterly upon request.
SYM004	RDBMS Patches / hotfix	Implementation of RDBMS patches and hotfixes.	Upon request.
SYM005	OS Patches	Implementation of OS patches.	Upon request

9.3 Supported Software

Service level guarantees apply only to vendor supplied and supported patches and the software that is provided as part of the Services. Customer must supply 3rd party software patches, (i.e. Oracle). Patching will only be provided for RHEL and SUSE Operating Systems with licences provided by Virtustream.

9.4 Untested Patches

At Customer's request, Virtustream will apply patches to Customer configuration. Virtustream makes no guaranty about the outcome of the application of an untested patch. If Customer would like a patch applied to their environment prior to the time that Virtustream would normally apply a patch (i.e., the

applicable patching window), Virtustream will do so within (4) four business day of the time the customer opens a support ticket requesting the application of the patch.

9.5 Release and Testing
Virtustream's default patching policy includes the application of all security related patches with the following ratings as defined by Microsoft Vulnerability Severity Ratings (Critical, Important, Moderate, Low) as well as all OS patches with a Critical Vulnerability Severity Rating. Patches are typically deployed within 7 days of "Patch Tuesday" as defined as the second Tuesday of the month, to Customer's development and or QA environments. Once patches are deployed the customer performs testing to ensure the patches do not cause any issues with their applications. After QA and development environments are deployed and no issues are discovered, the patching of the production environment will commence. Customer is responsible for turning off applications and databases, or providing pre and post scripts to allow Virtustream to turn off applications and databases.

Standard Support does not include testing prior to patching of the production environment. Patches for Standard Support will be automatically applied on the 3rd Sunday of each month.

Virtustream requires an open service request from customer to apply patches. This request must be received 5 business days prior to the approved patch window authorizing Virtustream to proceed. If any patches are to be excluded said patches must be noted in the Service Request.

70

EXHIBIT 6

CLOUD PLATFORM SERVICES
SERVICE DESCRIPTION for NASPO
March 2016

rev 1

NOTICE

Any performance data provided is based on relevant information made available to us at the present time, and must (except where stated otherwise) be regarded as an estimate only, since the actual performance and functionality of any computer system will depend upon a variety of factors, not all of which are related to the products and services that may ultimately be supplied.

All brands and products referenced in this Service Description are acknowledged to be trademarks or registered trademarks of their respective owners.

1   SERVICES OVERVIEW

This Service Description (SD) describes the Virtustream Cloud Platform Services (CPS) offerings. These services are hosted in secure Virtustream data centers in the United States, and comprise a range of Infrastructure as a Service (IaaS) platform capabilities, from compute, to storage, security, disaster recovery, and colocation.

In this overview section you will find a series of tables, broken out by category, that provide a listing, product ID, and brief description for each service. The categories are:

IaaS Services
- IaaS Onboarding and Migration
- IaaS Compute
- IaaS HANA Physical Appliances
- IaaS Software
- IaaS Storage / Backup
- IaaS Network
- IaaS Cloud & Storage Connect
- IaaS Ad Hoc Services

Security Services: Network Based (Perimeter Defense)
- Firewall
- IPSec VPN
- Intrusion Detection Service (IDS) - Network-level

Security Services: VM Based
- Anti-Virus / Anti-Malware (AV/AM) - VM-level
- Intrusion Detection Service (IDS) - VM-level
- File Integrity Monitoring (FIM)
- VM-Level Security Bundle (VLSB) - Includes AV/VM, IDS, and FIM
- Encryption
- Vulnerability Scanning
- Distributed Denial of Service (DDoS) Monitoring
- Vulnerability Scanning
- Log Management
- Security Policy Auditing
- Two-Factor Authentication (2FA)

Related Colocation Services
- US Data Centers: 1 and 2
- Remote Management

The next section, Detailed Service Descriptions, beginning on page 19, provides a more comprehensive description of each service, including billing parameters and dependencies on other services.

1.1   Assumptions

The delivery of the Virtustream Cloud Platform Services described in this Service Description are predicated on the following assumptions:

- Customer fulfills the responsibilities specified in this SD or reasonably requested by Virtustream.
- Customer will reasonably respond promptly to any Virtustream requests to provide direction, information, approvals, or decisions that are reasonably necessary to be provided by Customer for Virtustream to perform the Services; provided that Virtustream shall not be responsible for any delays in the Services to the extent Customer's response is delayed.
- Customer will ensure that all nominated Customer personnel who work on Virtustream's systems or equipment are adequately qualified and receive suitable training at Customer's expense both to ensure the safety of Customer's personnel, and to safeguard Virtustream's systems or equipment.
- Customer shall obtain all necessary licenses and permissions to use third party software (when such software is not directly provided by Virtustream as part of the Services) for the provision of the Services and, where necessary, access to the software, data, and other materials and modifications for the purposes of the provision of the Services.
- Customer shall ensure that it obtains all rights and permissions from vendors and other third parties as necessary to permit Virtustream to access the information and data to be made available to Virtustream as specified hereunder.

1.2   IaaS Services: Overview

The tables in this overview provide a brief list of the Virtustream CPS services. Each is listed with its product ID, name, and a short description. Additional information for each is available in the next section, Detailed Service Descriptions, starting on page 19.

A list of terms specific to how these services are named and described are defined below:

µVM. Pronounced "micro VM," this is Virtustream's fine-grained unit of measurement designed to accurately measure the actual consumption of cloud resources. A µVM is a unit of consumption of computing resources, measured by CPU, memory, storage IOPS, and associated local network bandwidth.

The usage of each µVM resource component (CPU, memory, storage input/output, and network bandwidth) is measured at five minute intervals — one unit each for 200MHz of CPU, 768MiB of memory, 40 storage input/output operations per second (IOPS), and 2Mbps of local network bandwidth. The highest of the four is averaged per hour, and the hour values averaged across the month to determine the overall µVM usage for the month.

> Note: The measurement is performed at the aggregate level — across Customer's entire µVM resource pool. Measured µVM bandwidth usage is only within the data center.

µVM Resource Pool. The aggregated physical compute hardware — CPU and memory, as well as other components — allocated to a set of µVMs in a Virtustream virtual infrastructure.

Primary and Secondary Data Centers. Each Virtustream customer's production work is hosted in one of Virtustream's secure data centers; that data center is then referred to as the customer's Primary data center. If the customer elects to reserve additional Virtustream resources to provide non-production compute resources and/or Disaster Recover (DR), those may be in a second Virtustream data center in an alternate geographic location; that data center is referred to as the customer's Secondary data center.

Basic and Reserve. These terms differentiate the two ways Virtustream offers µVMs services.

"Basic Plus" µVM services are limited to a single Virtustream data center and have 99.99% availability.

"Reserve" µVM services are reserved compute resources at the customer designated DR (AKA Seconday) Virtustream data center. Generally, an equivalent quantity of µVMs used for production workloads is reserved at Customer-designated secondary Virtustream data center for on-going operation during disaster events and during scheduled disaster recovery (DR) exercises.

In both cases, overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

Units of Capacity. Throughout this document, units of memory, disk, and network capacity are as follows:

Byte: **Byte (B)** = 1 Byte

Memory: **Mebibyte (MiB)**: 1 MiB = 2^{20} B = 1,048,576 B
              Gibibyte (GiB): 1 GiB = 2^{30} B = 1,073,741,824 B
              Tebibyte (TiB): 1 TiB = 2^{40} bytes = 1,099,511,627,776 bytes

Disk: **Megabyte (MB)**: 1 MB = 10^6 B = 1,000,000 B
              Gigabyte (GB): 1 GB = 10^9 B = 1,000,000,000 B
              Terabyte (TB): 1 TB = 10^{12} B = 1000000000000 B

Network: **Megabit per second (Mbps)**: 1,000,000 bits per second
              Gigabit per second (Gbps): 1,000,000,000 bits per second

High Memory. Virtustream offers competitive pricing on compute services for applications that require large amounts of memory (64GiB or more) and high µVM consumption (32 µVMs and above).

Project Based. A few of the services listed are highly variable in scope and customer need. These services are billed as "project based." For these services, Virtustream will gather the scope and requirements to satisfy the need in a specific customer engagement, and the project will be scheduled and billed in accordance with those requirements.

Additional terms can be found in Section 7, Definitions, starting on page 75.

Table 1-1. IaaS Onboarding and Migration			
Product ID	**Product Name**	**Billing**	**Description**
IC-ONB-VLED-1T	IaaS Onboarding - Virtustream Led	one time, per VM	Virtustream will provision platform resources and migrate Customer systems to the Virtustream cloud.
IC-ONB-SS-1T	IaaS Onboarding - Self-Service	one time, per VM	Virtustream will enable a secure connection to the Virtustream cloud and provision IaaS resources. After Virtustream-led training, Customer will migrate their systems to the Virtustream cloud.
IC-ONB-PROJ-1T	IaaS Onboarding - Project Based	per project	Virtustream will enable a secure connection to the Virtustream cloud and provision IaaS resources. All other responsibilities as agreed between Virtustream and Customer, per Customer requirements.
IC-MIG-PROJ-1T	IaaS Migration Support (IaaS Onboarding Charge) - Project Based	per project	Virtustream will assess Customer requirements, define a migration plan, and execute system migration, per plan.

Table 1-2. IaaS Compute			
Product ID	**Product Name**	**Billing**	**Description**
IC-uVM-BASP-ENT	Enterprise Basic Plus µVM	monthly, per usage	Enterprise Basic µVMs are used for non-production and production non-Internet-accessible workloads.
IC-uVM-RESV-ENT	Enterprise Reserve µVM	monthly, per usage	Enterprise Reserve µVMs are generally used for production, non-Internet-accessible workloads. An equivalent quantity of µVMs used for production workloads are reserved at a secondary Virtustream data center for ongoing operation in case of disaster events and during scheduled disaster recovery (DR) exercises.
HM-HA-VIR-1T	vHANA Installation and Setup Charge - Virtual Appliance	one time, per VM	Setup and configuration of the Virtual HANA managed appliance.
IC-HVM-BASP-ENT	High Memory Enterprise Basic Plus VM Fee	monthly, per VM	Surcharge Must be paired with *High Memory Enterprise Basic µVM Fee* (directly below).
IC-uHV-BASP-ENT	High Memory Enterprise Basi Plusc µVM	monthly, per usage	High Memory Enterprise Basic µVMs are recommended for >32 µVM workloads. Must be paired with *High Memory Enterprise Basic VM Fee* (directly above). Enterprise Basic µVMs are used for non-Internet-accessible workloads and can be used for vHANA.
IC-uHV-RESV-ENT	High Memory Enterprise Reserve µVM	monthly, per usage	High Memory Enterprise Reseve µVMs are recommended for >32 µVM workloads. Enterprise Resever µVMs are generally used for production, non-Internet-accessible workloads. An equivalent quantity of µVMs used for production workloads are reserved at a secondary Virtustream data center for ongoing operation during disaster events and during

Product ID	Product Name	Billing	Description
			scheduled disaster recovery (DR) exercises.

Table 1-3. IaaS HANA Physical Appliances			
Product ID	**Product Name**	**Billing**	**Description**
HM-HA-PHS-1T	HANA Appliance Installation and Setup - Physical Appliance	one time, per appliance	Setup and configuration of a Physical HANA managed appliance.
HM-HA-MIG-1T	HANA Migration and Optimization	per project	Migration and optimization of Customer's database into the HANA managed appliance.
HM-HA1-SOH-6TB	6 TB HANA Managed Appliance for SOH - Primary	monthly, per appliance	Dedicated 6TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
HM-HA2-SOH-6TB	6 TB HANA Managed Appliance for SOH - Secondary	monthly, per appliance	Dedicated 6TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
HM-HA1-SOH-3TB	3 TB HANA Managed Appliance for SOH - Primary	monthly, per appliance	Dedicated 3TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
HM-HA2-SOH-3TB	3 TB HANA Managed Appliance for SOH - Secondary	monthly, per appliance	Dedicated 3TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
HM-HA1-SN-2TB	2 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary	monthly, per appliance	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
HM-HA2-SN-2TB	2 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	monthly, per appliance	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's - Secondary Virtustream data center. (Hardware only.).
HM-HA1-SO-2TB	2 TB HANA Managed Appliance for BW (Scale-Out) - Primary	monthly, per appliance	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
HM-HA2-SO-2TB	2 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	monthly, per appliance	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
HM-HA1-SOH-2TB	2 TB HANA Managed Appliance for SOH - Primary	monthly, per appliance	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
HM-HA2-SOH-2TB	2 TB HANA Managed Appliance for SOH - Secondary	monthly, per appliance	Dedicated 2TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
HM-HA1-SOH-15TB	1.5 TB HANA Managed Appliance for SOH - Primary	monthly, per appliance	Dedicated 1.5TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
HM-HA2-SOH-15TB	1.5 TB HANA Managed Appliance for SOH - Secondary	monthly, per appliance	Dedicated 1.5TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).

Product ID	Product Name	Billing	Description
HM-HA1-SN-1TB	1 TB HANA Managed Appliance (Single-Node/Scale-Up) - Primary	monthly, per appliance	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
HM-HA2-SN-1TB	1 TB HANA Managed Appliance (Single-Node/Scale-Up) - Secondary	monthly, per appliance	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
HM-HA1-SO-1TB	1 TB HANA Managed Appliance for BW (Scale-Out) - Primary	monthly, per appliance	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
HM-HA2-SO-1TB	1 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	monthly, per appliance	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
HM-HA1-SOH-1TB	1 TB HANA Managed Appliance for SOH - Primary	monthly, per appliance	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
HM-HA2-SOH-1TB	1 TB HANA Managed Appliance for SOH - Secondary	monthly, per appliance	Dedicated 1TiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).
HM-HA1-SN-512	512 GB HANA Managed Appliance (Single-Node/Scale-Up) - Primary	monthly, per appliance	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.)
HM-HA2-SN-512	512 GB HANA Managed Appliance (Single-Node/Scale-Up) - Secondary	monthly, per appliance	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-up architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.)
HM-HA1-SO-512	512 GB HANA Managed Appliance for BW (Scale-Out) - Primary	monthly, per appliance	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Primary Virtustream data center. (Hardware only.).
HM-HA2-SO-512	512 GB HANA Managed Appliance for BW (Scale-Out) - Secondary	monthly, per appliance	Dedicated 512GiB HANA Managed Appliance that supports the HANA Scale-out architecture. Resides in Customer's Secondary Virtustream data center. (Hardware only.).

Table 1-4. OS, Database, and Other Software			
Product ID	Product Name	Billing	Description
IC-SW-MQL-STD	Microsoft SQL Standard (Per 2 cores)	monthly, per 2 cores	Microsoft SQL Server, Standard Edition license for unlimited users per month.
IC-SW-MQL-ENT	Microsoft SQL Enterprise (Per 2 cores)	monthly, per 2 cores	Microsoft SQL Server, Enterprise Edition license for unlimited users per month.
IC-SW-SLES-2C	SUSE Linux Enterprise ≤ 2 vCPU & ≤ 2GB RAM	monthly, per instance	SUSE Linux Enterprise Server for x86&x86-64, per hosted instance.

Product ID	Product Name	Billing	Description
IC-SW-SLES-4C	SUSE Linux Enterprise ≤ 4 vCPU & ≤ 8GB RAM	monthly, per instance	SUSE Linux Enterprise Server for x86&x86-64, hosted instance.
IC-SW-SLES-8C	SUSE Linux Enterprise ≤ 8 vCPU & > 8GB RAM	monthly, per instance	SUSE Linux Enterprise Server for x86&x86-64, hosted instance.
IC-SW-SLES-VCPU	SUSE Linux Enterprise > 8 vCPU or > 8GB RAM	monthly, per vCPU	SUSE Linux Enterprise Server for x86&x86-64.
IC-SW-SLES-S2C	SUSE Linux Enterprise for SAP ≤ 2 vCPU & ≤ 2GB RAM	monthly, per instance	SUSE Linux Enterprise Server for x86&x86-64, hosted instance. Optimized for use with SAP.
IC-SW-SLES-S4C	SUSE Linux Enterprise for SAP ≤ 4 vCPU & ≤ 8GB RAM	monthly, per instance	SUSE Linux Enterprise Server for x86&x86-64, hosted instance. Optimized for use with SAP.
IC-SW-SLES-SVM	SUSE Linux Enterprise for SAP > 4 vCPU or > 8GB RAM	monthly, per instance	SUSE Linux Enterprise Server for x86&x86-64, hosted instance. Optimized for use with SAP.
IC-SW-SLES-PH	SUSE Linux Enterprise for Physical HANA	monthly, per socket pair	SUSE Linux Enterprise Server for x86&x86-64. For use on physical HANA appliances.
IC-SW-RHL-STD	Red Hat Enterprise Linux - Standard (Per OS)	monthly, per instance	Red Hat Enterprise Linux, Standard, for four or fewer vCPUs.
IC-SW-RHL-ENT	Red Hat Enterprise Linux – Enterprise (Per OS)	monthly, per instance	Red Hat Enterprise Linux, Enterprise, for five or more vCPUs.
IC-SW-MSS-WIN	Microsoft OS	monthly, per instance	Windows Server OS.
IC-SW-RDS-IF	Remote Desktop Services (Per User)	monthly, per user	Allows an end user to access a Microsoft Remote Desktop session host running on the Virtustream cloud platform.

Table 1-5. IaaS Storage & Backup			
Product ID	**Product Name**	**Billing**	**Description**
IC-DP-BU-1T	System Backup Setup	one time, per account	Setup and configuration of Customer's backup environment.
IC-DP-BUP-REP	STANDARD System Backup (PROTECTED) - Replicated	monthly, per GB protected	File system backup at Customer's primary Virtustream data center on a periodic basis. Backups are replicated to Customer's secondary Virtustream data center.
IC-DP-BUP-LOC	STANDARD System Backup (PROTECTED) - Local Only	monthly, per GB protected	File system backup at Customer's primary Virtustream data center on a periodic basis.
IC-DP-BUPH-REP	HANA System Backup (Protected Data) - Replicated	monthly, per GB protected	File system backup at Customer's primary Virtustream data center on a periodic basis for HANA. Backups are replicated to Customer's secondary Virtustream data center.
IC-DP-BUPH-LOC	HANA System Backup (Protected Data) – Local Only	monthly, per GB protected	File system backup at Customer's primary Virtustream data center on a periodic basis for HANA.

Product ID	Product Name	Billing	Description
IC-DP-BU-ARCH	Archive Storage	project based	Long-term archive storage, off-Site.
IC-STO-T0A-LOC	Tier 0 Block Storage – Local Only	monthly, per GB allocated	Tier 0 local block Storage with 3ms Latency Service Level, maintained in a single data center.
IC-STO-T1A-LOC	Tier I Block Storage – Local Only	monthly, per GB allocated	Tier I local block Storage with 10ms Latency Service Level, maintained in a single data center.
IC-STO-T2A-LOC	Tier II Block Storage – Local Only	monthly, per GB allocated	Tier II local block Storage with 20ms Latency Service Level, maintained in a single data center.
IC-STO-T3A-LOC	Tier III Block Storage – Local Only	monthly, per GB allocated	Tier III local block Storage w/ 40ms Latency Service Objective, maintained in a single data center.
IC-STO-T0A-REP	Tier 0 Block Storage – Replicated	monthly, per GB allocated	Tier 0 replicated block Storage w/ 3ms Latency Service Level persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.
IC-STO-T1A-REP	Tier I Block Storage – Replicated	monthly, per GB allocated	Tier I replicated block Storage w/ 10ms Latency Service Level persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.
IC-STO-T2A-REP	Tier II Block Storage – Replicated	monthly, per GB allocated	Tier II replicated block Storage w/ 20ms Latency Service Level persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.
IC-STO-T3A-REP	Tier III Block Storage – Replicated	monthly, per GB allocated	Tier III replicated block Storage w/ 40ms Latency Service Objective persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Table 1-6. IaaS Network			
Product ID	Product Name	Billing	Description
IC-NW-BWU1-NET	Network Bandwidth Fee - USDC1	monthly, per Mbps	Internet-facing bandwidth to/from Virtustream's Washington, DC data center.
IC-NW-BWU2-NET	Network Bandwidth Fee - USDC2	monthly, per Mbps	Internet-facing bandwidth to/from Virtustream's San Francisco, CA data center.
IC-NW-BWU3-NET	Network Bandwidth Fee - USDC3	monthly, per Mbps	Internet-facing bandwidth to/from Virtustream's Las Vegas, NV data center.
IC-NW-BWG1-NET	Network Bandwidth Fee - UKDC1	monthly, per Mbps	Internet-facing bandwidth to/from Virtustream's UK data center.
IC-NW-BWG3-NET	Network Bandwidth Fee – NLDC1	monthly, per Mbps	Internet-facing bandwidth to/from Virtustream's NL data center.
IC-NW-IPAD-V6	Public IP Address (IPv6)	monthly, per address	Per assigned public IPv6 IP address block per month.
IC-NW-IPAD-V4	Public IP Address	monthly,	Per assigned public IPv4 IP address per month.

Product ID	Product Name	Billing	Description
	(IPv4)	per address	

Table 1-7. IaaS Load Balancer			
Product ID	**Product Name**	**Billing**	**Description**
IC-NW-LBB-1T	Load Balancer Setup – Basic	one time, per instance	Template provided to Customer for service list and rule preferences; Virtustream configures.
IC-NW-LBA-1T	Load Balancer Setup - Advanced	one time, per instance	Technical briefing with Customer to determine sizing and level of effort.
IC-NW-LBM-NET	Load Balancing Fee (Additional to Network Bandwidth)	monthly, per Mbps	Fee for load balancer bandwidth use.
IC-NW-LBM-LB	Managed Load Balancer Services (Per Server)	monthly, per VM in DMZ	Virtustream-managed load balancer facilitates Customer load balancer configuration change requests.

Table 1-8. IaaS Cloud & Storage Connect			
Product ID	**Product Name**	**Billing**	**Description**
Cloud Connect, USDC1 - Washington, DC			
DC-NWU1-XCS-1T	Cloud Connect - Standard (24 ports available) - Setup - USDC1	one time, per instance	Installation of one 24-port, gigabit network switch in Virtustream's Washington, DC data center.
DC-NWU1-XCS-STD	Cloud Connect - Standard (24 ports available) - USDC1	monthly, per instance	One 24-port gigabit network switch providing colocation-to-cloud connectivity in Virtustream's Washington, DC data center.
DC-NWU1-XCH-1T	Cloud Connect - HA (48 ports available) - Setup - USDC1	one time, per instance	Installation of two 24-port, gigabit network switches (for High Availability) in Virtustream's Washington, DC data center.
DC-NWU1-XCH-HA	Cloud Connect - HA (48 ports available) - USDC1	monthly, per instance	Two managed, 24-port gigabit network switches (for a total of 48 ports) providing High Availability (HA) colocation-to-cloud connectivity in Virtustream's Washington, DC data center.
Cloud Connect, USDC2 - San Francisco, CA			
DC-NWU2-XCS-1T	Cloud Connect - Standard (24 ports available) - Setup - USDC2	one time, per instance	Installation of one 24-port, gigabit network switch in Virtustream's San Francisco, CA data center.
DC-NWU2-XCS-STD	Cloud Connect - Standard (24 ports available) - USDC2	monthly, per instance	One 24-port gigabit network switch providing colocation-to-cloud connectivity Virtustream's San Francisco, CA data center.
DC-NWU2-XCH-1T	Cloud Connect - HA (48 ports available) - Setup - USDC2	one time, per instance	Installation of two 24-port, gigabit network switches (for High Availability) Virtustream's San Francisco, CA data center.
DC-NWU2-XCH-HA	Cloud Connect - HA (48 ports available) - USDC2	monthly, per instance	Two managed, 24-port gigabit network switches (for a total of 48 ports) providing High Availability (HA) colocation-to-cloud connectivity Virtustream's San Francisco, CA data center.

Product ID	Product Name	Billing	Description
Storage Connect, USDC1 - Washington, DC			
DC-NWU1-SCS-1T	Storage Connect - Standard - Setup - USDC1	one time, per instance	Installation of one Fiber Channel switch in Virtustream's Washington, DC data center.
DC-NWU1-SCS-STD	Storage Connect - Standard - USDC1	monthly, per instance	Single Fiber Channel switch providing Storage connectivity in Virtustream's Washington, DC data center.
DC-NWU1-SCH-1T	Storage Connect - HA - Setup - USDC1	one time, per instance	Installation of two Fiber Channel switches in Virtustream's Washington, DC data center.
DC-NWU1-SCH-HA	Storage Connect - HA - USDC1	monthly, per instance	Dual Fiber Channel switches providing Storage connectivity in Virtustream's Washington, DC data center.
Storage Connect, USDC2 - San Francisco, CA			
DC-NWU2-SCS-1T	Storage Connect - Standard - Setup - USDC2	one time, per instance	Installation of one Fiber Channel switch in Virtustream's San Francisco, VA data center.
DC-NWU2-SCS-STD	Storage Connect - Standard - USDC2	monthly, per instance	Single Fiber Channel switch providing Storage connectivity San Francisco, VA data center.
DC-NWU2-SCH-1T	Storage Connect - HA - Setup - USDC2	one time, per instance	Installation of two Fiber Channel switches San Francisco, VA data center.
DC-NWU2-SCH-HA	Storage Connect - HA - USDC2	monthly, per instance	Dual Fiber Channel switches providing Storage connectivity San Francisco, VA data center.

Table 1-9. IaaS Ad Hoc Services			
Product ID	**Product Name**	**Billing**	**Description**
IC-SVC-DR-PROJ	DR Test Planning	Project based	Disaster Recovery (DR) Test Planning process produces Customer-specific DR Test Plan that specifies the scope of VMs, VLANs, and Storage (Data Stores) to be tested, is specific to the customer environment, and can be conducted with minimal disruption to the customer's on-going production workload.
IC-SVC-DR1-AH	DR Test Service Tier 1 (10 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 10 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR2-AH	DR Test Service Tier 2 (20 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 20 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR3-AH	DR Test Service Tier 3 (40 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 40 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR4-AH	DR Test Service Tier 4 (80 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 80 VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR5-AH	DR Test Service Tier 5 (160 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 160VMs. (One VLAN per five VMs; one Data Store per two VMs.)
IC-SVC-DR6-AH	DR Test Service Tier 6 (320 VMs)	one time, per test	Disaster Recovery test using pre-existing DR Test Plan for up to 320 VMs. (One VLAN per five VMs; one Data Store per two VMs.)

Product ID	Product Name	Billing	Description
IC-RPT-VRS-REQ	Virtualization Right Sizing Report	one time, per report	Right Sizing report showing configured versus actual usage with recommendations on CPU and memory for up to 500 VMs.
IC-RPT-VCC-REQ	Virtualization Custom Consumption Report	one time, per report	Custom consumption report for up to 500 VMs showing compute and storage utilization broken down by VM and resource pool.
IC-DP-BU-CRS	Backup Restoration Request with CCS	one time, per restoration	Additional Backup Restorations beyond the included 10-per-month; for Customers with Virtustream Cloud Cover Services.
IC-DP-BU-NRS	Backup Restoration Request without CCS	one time, per restoration	Additional Backup Restorations beyond the included 10-per-month; for customers without Virtustream Cloud Cover Services.

1.3   Security Services - Network Based (Perimeter Defense): Overview

Table 1-10. Firewall			
Product ID	Product Name	Billing	Description
CS-FW-FW-1T	Firewall Configuration/Setup	one time, per firewall	Firewall configuration and setup fee; required for each location with Internet-facing bandwidth.
CS-FW-MPF-SVC	Managed Perimeter Firewall	monthly, per VM	Virtustream-managed firewall service facilitates Customer firewall configuration change requests.

Table 1-11. IPSec VPN			
Product ID	Product Name	Billing	Description
CS-VPN-H-1T	IPSec VPN Host-Side Configuration	one time, per VPN tunnel	IPSec VPN Tunnel configuration/management at the Virtustream data center.
CS-VPN-C-1T	IPSec VPN Client-Side Configuration	one time, per VPN tunnel	Remote support of Customer's configuration of the IPSec VPN Tunnel at Customer site.
CS-VPN-U1-NET	IPSec VPN Bandwidth Fee - USDC1	monthly, per Mbps	IPSec VPN Bandwidth between Customer site and Virtustream's Washington, DC Data Center.
CS-VPN-U2-NET	IPSec VPN Bandwidth Fee - USDC2	monthly, per Mbps	IPSec VPN Bandwidth between Customer site and Virtustream's San Francisco, CA Data Center.
CS-VPN-U3-NET	IPSec VPN Bandwidth Fee - USDC3	monthly, per Mbps	IPSec VPN Bandwidth between Customer site and Virtustream's Las Vegas, NV Data Center.
CS-VPN-G1-NET	IPSec VPN Bandwidth Fee - UKDC1	monthly, per Mbps	IPSec VPN Bandwidth between Customer site and Virtustream's London Data Center.
CS-VPN-G3-NET	IPSec VPN Bandwidth Fee - NLDC1	monthly, per Mbps	IPSec VPN Bandwidth between Customer site and Virtustream's Amsterdam Data Center.
CS-VPN-T-SVC	VPN Tunnel Managed Service Fee	monthly, per VPN tunnel	Maintenance of circuit between Virtustream data center and Customer's facility.

Table 1-12. Intrusion Detection Service (IDS) - Network-based			
Product ID	**Product Name**	**Billing**	**Description**
CS-IDS-NB1-1T	Network Based Intrusion Detection Primary Site Setup	one time, per vLAN	Intrusion Detection Services (IDS) installation and configuration at Customer's primary Virtustream data center.
CS-IDS-NB1-1T-SYS	Network Based Intrusion Detection System and Managed Service Fee - Primary	monthly, per vLAN	Managed service for the network-based Intrusion Detection Service (IDS) at Customer's primary Virtustream data center.
CS-IDS-NB2-1T	Network Based Intrusion Detection Second Site Setup	one time, per vLAN	Intrusion Detection Services (IDS) installation and configuration at Customer's secondary Virtustream data center.
CS-IDS-NB2-SYS	Network Based Intrusion Detection System & Managed Service Fee - Secondary	monthly, per vLAN	Managed service for the network-based Intrusion Detection Service (IDS) at Customer's secondary Virtustream data center.

1.4   Security Services - VM-Level: Overview

Table 1-13. Anti-Virus / Anti-Malware (AV/AM) - VM-based			
Product ID	**Product Name**	**Billing**	**Description**
CS-TM-AV-1T	Anti-Virus Primary System Setup	one time, per account	Virtustream will deploy an anti-virus / anti-malware system to Customer specifications in Customer's primary Virtustream data center.
CS-TM-AV-SYS	Anti-Virus Primary System	monthly, per account	Includes threat updates, patches, minor service pack releases, and major system upgrades for the AV / AM system at Customer's primary Virtustream data center.
CS-TM-AV-1T	Anti-Virus Secondary System Setup	one time, per account	Virtustream will deploy an anti-virus / anti-malware system to Customer specifications in Customer's secondary Virtustream data center.
CS-TM-AV1-SVC	Anti-Virus Secondary System	monthly, per account	Includes threat updates, patches, minor service pack releases, and major system upgrades for the AV / AM system at Customer's secondary Virtustream data center.

Table 1-14. Intrusion Detection Service (IDS) - VM-based			
Product ID	**Product Name**	**Billing**	**Description**
CS-TM-IDFW-1T	Intrusion Detection and Firewall Primary System Setup	one time, per account	Setup of VM-level IDS and firewall in Customer's primary Virtustream data center.
CS-TM-IDFW-SYS	Intrusion Detection and Firewall Primary System	monthly, per account	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the IDS system at Customer's primary Virtustream data center.
CS-TM-IDFW-1T	Intrusion Detection and Firewall Secondary System Setup	one time, per account	Setup of VM-level IDS and firewall in Customer's secondary Virtustream data center.

Product ID	Product Name	Billing	Description
CS-TM-IDFW-SYS	Intrusion Detection and Firewall Secondary System	monthly, per account	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the IDS system at Customer's secondary Virtustream data center.
CS-TM-IDFW1-SVC	Intrusion Detection and Firewall Managed Service	monthly, per VM	Virtustream manages all IDS and firewall rule change requests.

Table 1-15. File Integrity Monitoring (FIM)			
Product ID	Product Name	Billing	Description
CS-TM-FIM-1T	File Integrity Monitoring Primary System Setup	one time, per account	Virtustream will install and configure a single instance of File Integrity Manager (FIM) at Customer's primary Virtustream data center based on Customer specifications.
CS-TM-FIM-SYS	File Integrity Monitoring Primary System	monthly, per account	Includes patches, minor service pack releases, and major system upgrades for the FIM system at Customer's primary Virtustream data center.
CS-TM-FIM-1T	File Integrity Monitoring Secondary System Setup	one time, per account	Virtustream will install and configure a single instance of File Integrity Manager (FIM) at Customer's secondary Virtustream data center based on Customer specifications.
CS-TM-FIM-SYS	File Integrity Monitoring Secondary System	monthly, per account	Includes patches, minor service pack releases, and major system upgrades for the FIM system at Customer's secondary Virtustream data center.
CS-TM-FIM1-SVC	File Integrity Monitoring Managed Service	monthly, per VM	Virtustream will monitor Customer's VMs and notify Customer of alerts generated by the FIM.

Table 1-16. VM-Level Security Bundle (VLSB)			
Product ID	Product Name	Billing	Description
CS-TM-VLSB1-1T	VM-Level Security Bundle Primary System Setup	one time, per account	Virtustream will consult with Customer, then deploy a Customer specific environment and with a Customer-specific policy configuration in Customer's primary Virtustream data center.
CS-TM-VLSB1-SYS	VM-Level Security Bundle Primary System fee	monthly, per account	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the VLSB system at Customer's primary Virtustream data center.
CS-TM-VLSB2-1T	VM-Level Security Bundle Secondary System Setup	one time, per account	Virtustream will consult with Customer, then deploy a Customer specific environment and with a Customer-specific policy configuration in Customer's secondary Virtustream data center.
CS-TM-VLSB2-SYS	VM-Level Security Bundle Secondary System fee	monthly, per account	Includes threat updates, patches, minor service pack releases, major system upgrades, and firewall rule changes for the VLSB system at Customer's secondary Virtustream data center.
CS-TM-VLSBA-SVC	VM-Level Security Bundle Service Fee (<101 VMs)	monthly, for 1-100 VMs	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.

Product ID	Product Name	Billing	Description
CS-TM-VLSBB-SVC	VM-Level Security Bundle Service Fee (<1,001 VMs)	monthly, for 101-1,000 VMs	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.
CS-TM-VLSBC-SVC	VM-Level Security Bundle Service Fee (<10,001 VMs)	monthly, for 1,001-10,000 VMs	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.
CS-TM-VLSBD-SVC	VM-Level Security Bundle Service Fee (>10,000 VMs)	monthly, for 10,001+ VMs	Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.

Table 1-17. Encryption			
Product ID	Product Name	Billing	Description
CS-ENC-SYSS-1T	Encryption Management System Setup - SaaS	one time, per account	Configuration of Customer in shared encryption system to manage encryption agents.
CS-ENC-SYSD-1T	Encryption Management System Setup - Dedicated	one time, per account	Setup and configuration of a Customer-specific, dedicated encryption system to manage encryption agents.
CS-ENC-SYS-SYS	Encryption Management System Fee	monthly, per system	Virtustream will monitor the operation of the encryption service and monitor for exceptions.
CS-ENC-AGT-1T	Encryption Agent Setup	one time, per VM	Setup encryption agent for each VM. Agents enforce the encryption policy as defined in the encryption management system.
CS-ENC-AGTC-PR	Encryption Production Agent per vCPU Fee	monthly, per vCPU	Fee covers agents in Customer's production environment.
CS-ENC-AGTC-NP	Encryption Non-Production Agent per vCPU Fee	monthly, per vCPU	Fee covers agents in Customer's non-production environment.
CS-ENC-AGTH-1T	HANA Encryption Agent Setup	one time, per appliance	Setup encryption agent for each HANA Appliance. Agents enforce the encryption policy as defined in the encryption management system.
CS-ENC-AGTH-PR	HANA Encryption Agent Fee (Production)	monthly, per 16 cores / vCPU	Fee covers agents on HANA appliances in Customer's production environment.
CS-ENC-AGTH-NP	HANA Encryption Agent Fee (Non-Production)	monthly, per 16 cores / vCPU	Fee covers agents on HANA appliances in Customer's non-production environment.
CS-ENC-AGTM-1T	High Memory Encryption Agent Setup	one time, per VM	Setup encryption agent for each High Memory VM. Agents enforce the encryption policy as defined in the encryption management system.
CS-ENC-AGTM-PR	High Memory Encryption Agent Fee (Production)	monthly, per vCPU	Fee covers agents on High Memory µVMs in Customer's production environment.
CS-ENC-AGTM-NP	High Memory Encryption Agent Fee (Non-Production)	monthly, per vCPU	Fee covers agents on High Memory µVMs in Customer's non-production environment.

Product ID	Product Name	Billing	Description
CS-ENC-AGTV-PR	Encryption Production Agent per VM Fee	Per VM	
CS-ENC-AGTV-NP	Encryption Non-Production Agent per VM Fee	Per VM	

Table 1-18. Vulnerability Scanning			
Product ID	Product Name	Billing	Description
CS-VS-NPIP-SVC	Vulnerability Scanning Managed Service - non Public IP	monthly, per non-public IP address	Scanning of non-public IP endpoints within the customer's Virtustream environment; generates reports on possible network vulnerabilities. Virtustream security personnel will provide monthly feedback and suggested prioritization of issues.
CS-VS-PIP-SVC	Vulnerability Scanning Managed Service - Public IP	monthly, per public IP address	Scanning of public IP endpoints within the customer's Virtustream environment; generates reports on possible network vulnerabilities. Virtustream security personnel will provide monthly feedback and suggested prioritization of issues.

Table 1-19. Distributed Denial of Service (DDoS) Monitoring			
Product ID	Product Name	Billing	Description
CS-DDOS-MR-1T	DDoS Monitoring and Reporting (5 Public IP Addresses) - Setup	one time, per 5 public IP addresses	Distributed Denial of Service (DDoS) monitoring and reporting setup and configuration.
CS-DDOS-MR-SVC	DDoS Monitoring and Reporting (5 Public IP Addresses)	monthly, per 5 public IP addresses	Distributed Denial of Service monitoring and reporting, including alerts and monthly statistics.

Table 1-20. Log Management			
Product ID	Product Name	Billing	Description
CS-VS-LM-1T	Log Management System Setup	one time, per system	Configuration of the Log Management System to support log management requirements.
CS-VS-MLM-1T	Managed Log Management Service Setup	one time, per VM	Installation and configuration of the log management system.
CS-VS-LM-SYS	Log Management System Fee	monthly, per system	Fee for monthly management of the log aggregation system.
CS-VS-MLM-SVC	Managed Log Management Service	monthly, per VM	Service fee for monthly management and monitoring of log aggregation system use, including log capacity recommendations.

Table 1-21. Security Policy Audit Services			
Product ID	Product Name	Billing	Description
CS-FA-FA-1T	Firewall Audit System Setup	one time, per account	Virtustream installation and configuration of the Firewall Audit Management System.

Product ID	Product Name	Billing	Description
CS-FA-FAE-1T	Firewall Audit Export Setup	one time, per firewall	Configuration and testing of Customer designated firewall in the Virtustream cloud to export settings to the Firewall Audit Manager.
CS-FA-FA-SYS	Firewall Audit System	monthly, per account	Virtustream maintenance of the Firewall Audit system, which monitors changes to the network security policy and provides a complete audit trail.
CS-VS-MFA-SVC	Managed Firewall Auditing Service	monthly, per firewall	Virtustream will the export the data from managed firewalls on a monthly basis, and perform analysis of supported firewalls as a scheduled audit.
CS-VS-PSYS-1T	Policy Auditor System Setup	one time, per system	Service includes the tasks necessary to install a dedicated FWPA system within the Customer's environment
CS-VS-PSVC-1T	Policy Auditor Service Setup	one time, per VM	Service includes the tasks required to configure a customer in either the Shared Firewall Policy Auditing System or a Dedicated Policy Auditor System.
CS-VS-PA-SYS	Policy Auditor System Fee	monthly, per system	This fee covers compute resources to support the Dedicated Policy Auditor deployment, including VM, OS, Memory, I/O, Storage, networking.
CS-VS-PA-SVC	Policy Auditor Service Fee	monthly, per VM	Fee for the performance of the firewall policy analysis. Deliverables include: Risky Rule report, Rule Optimization Report, PCI Compliance Report.

Table 1-22. Two-Factor Authentication (2FA)			
Product ID	Product Name	Billing	Description
CS-2F-VPT-1T	2FA Virtustream Portal Token Issue	one time, per user	Virtustream will register a 2FA token for the Virtustream Portal, and provide users with information and, when necessary, training for how to use tokens.
CS-2F-VPT-MF	2FA Virtustream Portal Token Fee	monthly, per user	Fee for ongoing use of each 2FA token for the Virtustream Portal.
CS-2F-D1-1T	2FA Dedicated Setup	one time, per instance	Virtustream will install and configure a single instance of 2FA management system on a per Tenant basis.
CS-2F-DS-1T	2FA Dedicated Self-Service Setup	one time, per instance	Customer will install and configure a single instance of the 2FA Management System on a per Tenant basis.
CS-2F-D1-SYS	2FA Dedicated Base Fee	monthly, per instance	Monthly fee for a single instance of a Customer's dedicated 2FA Management System at Customer's primary Virtustream data center.
CS-2F-D2-1T	2FA Dedicated DR Setup	one time, per instance	Virtustream will install and configure a single instance of the 2FA Management System on a per Tenant basis in Customer's secondary Virtustream data center.
CS-2F-D2-SYS	2FA Dedicated DR Base Fee	monthly, per instance	Monthly fee for a single instance of a Customer's dedicated 2FA Management System at Customer's secondary Virtustream data center.
CS-2F-DT-1T	2FA Dedicated Token Issue	one time, per user	Customer personnel will issue and install a 2FA token on a mobile device or computer.
CS-2F-DT-MF	2FA Dedicated Token Fee	monthly, per user	Monthly fee for the use of 2FA Tokens associated with the 2FA Management System.
CS-2F-S-1T	2FA Shared Setup	one time, per instance	Virtustream will assist Customer in setting up an account in Virtustream's Shared 2FA Management System.

Product ID	Product Name	Billing	Description
CS-2F-SS-1T	2FA Shared Self-Service Setup	one time, per instance	Customer will set up an account in Virtustream's Shared 2FA Management System. Virtustream will supply Customer with information required to integrate to Customer's designated Active Directory (AD).
CS-2F-ST-1T	2FA Shared Token Issue	one time, per user	Customer personnel will issue and install an 2FA token on a mobile device or computer.
CS-2F-ST-MF	2FA Shared Token Fee	monthly, per user	Monthly fee for the use of 2FA Tokens associated with the 2FA Management System.

1.5   Colocation Services: Overview

Table 1-23. Colocation Services			
Product ID	Product Name	Billing	Description
Colocation Services, USDC1 - Washington, DC			
DC-NWU1-XCF-1T	Fiber Cross Connect - Vienna - Installation	one time, per project	Fiber Cross Connect Installation - Washington, DC data center.
DC-NWU1-XCC-1T	Copper Cross Connect - Vienna - Installation	one time, per project	Copper Cross Connect Installation - Washington, DC data center.
DC-NWU1-XCF-MF	Fiber Cross Connect - Vienna	monthly, each	Fiber Cross Connect - Washington, DC data center.
DC-NWU1-XCC-MF	Copper Cross Connect - Vienna	monthly, each	Copper Cross Connect - Washington, DC data center.
DC-RKU1-RK-HR	Hotel Rack (1U) - Managed Colo - Vienna	monthly, per rack unit	2x 1G Copper interfaces per RU - Washington, DC data center; Remote Eyes & Hands required: DC-SVC-REU-B, -S, or -G.
Colocation Services, USDC2 - San Francisco, CA			
DC-NWU2-XCF-1T	Fiber Cross Connect - San Francisco - Installation	one time, per project	Fiber Cross Connect Installation - San Francisco, CA data center.
DC-NWU2-XCC-1T	Copper Cross Connect - San Francisco - Installation	one time, per project	Copper Cross Connect Installation - San Francisco, CA data center.
DC-NWU2-XCF-MF	Fiber Cross Connect - San Francisco	monthly, each	Fiber Cross Connect - San Francisco, CA data center.
DC-NWU2-XCC-MF	Copper Cross Connect - San Francisco	monthly, each	Copper Cross Connect - San Francisco, CA data center.
DC-RKU2-RK-HR	Hotel Rack (1U) - Managed Colo - San Francisco	monthly, per rack unit	2x 1G Copper interfaces per RU; Remote Eyes & Hands required: DC-SVC-REU-B, -S, or -G
Remote Eyes & Hands			
DC-SVC-REU-B	Remote Eyes & Hands (US) - Bronze	monthly	Bronze (9x5) 2 hours (Billed in 15 min increments).

Product ID	Product Name	Billing	Description
DC-SVC-REU-S	Remote Eyes & Hands (US) - Silver	monthly	Silver (9x5) 5 hours (Billed in 15 min increments).
DC-SVC-REU-G	Remote Eyes & Hands (US) - Gold	monthly	Gold (24x7) 10 hours.
DC-SVC-REU-SAHQ	Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (15 Minutes)	services	15-minute increment of US Bronze or Silver service
DC-SVC-REU-SAH1	Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (1 Hour)	services	1-hour increment of US Bronze or Silver service
DC-SVC-REU-GAHQ	Remote Eyes & Hands (US) - Gold Ad Hoc (15 Minutes)	services	15-minute increment of US Gold service
DC-SVC-REU-GAH1	Remote Eyes & Hands (US) - Gold Ad Hoc (1 Hour)	services	1-hour increment of US Gold service
DC-SVC-REG-G	Remote Eyes & Hands (UK) - Gold	monthly	Gold (24x7) 10 hours.

2 DETAILED SERVICE DESCRIPTIONS

2.1 IaaS Services

2.1.1 IaaS Onboarding and Migration

2.1.1.1 IaaS Onboarding - Virtustream Led (IC-ONB-VLED-1T)

Virtustream will be responsible for provisioning the Virtustream IaaS Platform resources, project management, system migration, and environment architecture. Customer will provide information and support as required. All application installation, troubleshooting, and configuration is Customer's responsibility unless specifically contracted and scoped to be the responsibility of Virtustream personnel in the applicable Order Form.

If the Virtustream services provided include Two-Factor Authentication (2FA), then Onboarding includes issuance of two 2FA tokens.

Billing. One-time charge, per VM.

Table 2-1. Onboarding Responsibilities, Virtustream Led		
Task	Customer	Virtustream
Platform Migration and Production Readiness		
Define scope of engagement.	R	R
Provide detailed requirements for VMs and/or source files.	R	S
Project management / coordination.	C	R
Create client network(s), connections and firewall contexts.	C	R
Provision cloud resources, including compute, Storage, and xStream.	C	R
Create templates for new VMs or VMs from source files.	C	R
Setup basic monitoring.	C	R
Migrate data / VM source files for testing.	S	R
Install / configure applications and application connectivity.	R	S
Replicate data for production cutover.	S	R
Execute technical cutover (final data / networking).	S	R
Troubleshoot application issues.	R	S
Workload planning and stress testing (if applicable).	R	S

R: Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
A: Accountable is the authority who approves the work of R before it is effective.
S: Support R as necessary to complete the task or deliverable.
C: Consulted reviews output or progress necessary to complete the task or deliverable.
I: Informed needs to be notified of results, completion, or deliverable but need not necessarily be consulted.
NOTE: When Virtustream is In the Support role or Consulted, Virtustream may charge Customer T&M for resources used.

2.1.1.2 IaaS Onboarding - Self Service (IC-ONB-SS-1T)

Virtustream will enable secure access to the Virtustream IaaS Platform and will provision the resources detailed in the applicable Order Form on the Virtustream Cloud Platform. A training session covering the xStream Portal will be scheduled by Virtustream, approved by Customer and carried out by Virtustream, after which Customer can create new machines or upload existing machines to the

Virtustream IaaS Platform without requiring assistance from or coordination with Virtustream. VM creation, data transfer, and cutover operations are solely the responsibility of Customer.

The parties' responsibilities in connection with self-service onboarding process are summarized in the table below. In addition, Virtustream will assist in provisioning the environment and provide support where needed in transferring Customer data to the xStream Platform and offer best practice advice.

Billing. One-time charge, per account.

Table 2-2. Onboarding Responsibilities, Self Service		
Task	Customer	Virtustream
Platform Migration and Production Readiness		
Define scope of engagement.	R	C
Provide detailed requirements for VMs and/or source files.	R	C
Project management / coordination.	R	C
Create client network(s), connections and firewall contexts.	C	R
Procure, deploy, and monitor the connection between Customer and Virtustream's data center. This comprises managing the routers on each end as well as the circuit.	R	C
Provision cloud resources, including compute, Storage, and xStream.	C	R
Create templates for new VMs or VMs from source files.	C	R
Setup basic monitoring.	C	R
Migrate data/VM source files for testing.	R	S
Install / configure applications and application connectivity.	R	
Replicate data for production cutover.	R	S
Execute technical cutover (final data / networking).	R	S
Troubleshoot application issues.	R	C
Workload planning and stress testing (if applicable).	R	S

R: Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
A: Accountable is the authority who approves the work of R before it is effective.
S: Support R as necessary to complete the task or deliverable.
C: Consulted reviews output or progress necessary to complete the task or deliverable.
I: Informed needs to be notified of results, completion, or deliverable but need not necessarily be consulted.
NOTE: When Virtustream is In the Support role or Consulted, Virtustream may charge Customer T&M for resources used.

2.1.1.3   IaaS Onboarding - Project Based (IC-ONB-PROJ-1T)

Virtustream will be responsible for enabling secure connection to the Virtustream IaaS cloud and the provisioning of necessary Virtustream resources. All other roles and responsibilities will be determined and agreed upon at the time of project kickoff between Customer's technical resources and Virtustream onboarding resources.

Billing. One-time charge, per agreed upon onboarding services based on Customer requirements.

2.1.1.4   IaaS Migration Support (IaaS Onboarding Charge) - Project Based (IC- MIG-PROJ-1T)

Based on Customer input, Virtustream will assess Customer's migration needs, define a plan and schedule, and execute against the plan.

Billing. One-time charge based on Virtustream assessment of Customer requirements.

Virtustream IaaS Compute is comprised of computing resources hosted in secure data centers that replace the physical computing hardware traditionally housed on Customer site. These resources include physical servers which are logically divided into VMs (virtual machines), each with an allocation of CPU and memory, and linked to storage.

Terms used in the detailed descriptions below:

µVM. Pronounced "micro VM," this is Virtustream's fine-grained unit of measurement designed to accurately measure the actual consumption of cloud resources. A µVM is a unit of computing resources, comprised of CPU, memory, storage IOPS, and associated local network bandwidth.

The usage of each µVM resource component (CPU, memory, storage input/output, and network bandwidth) is measured at five minute intervals — one unit each for 200MHz of CPU, 768MiB of memory, 40 storage fabric input/output operations per second (IOPS), and 2Mbps of local network bandwidth. The highest of the four is averaged per hour, and the hour values averaged across the month to determine the overall µVM usage for the month.

> Note: The measurement is performed at the aggregate level — across Customer's entire µVM resource pool. Bandwidth usage is only within the data center.

Primary and Secondary Data Centers. Virtustream will work with Customer to select the Virtustream data center that will be identified as the "Primary" data center. If Customer has a requirement to host workloads in a separate data center, Virtustream will work with Customer to identify the Virtustream data center that will be identified as the "Secondary" data center.
In most cases, the Primary data center will host production workloads and the Secondary data center will serve as the DR target and may host non-production workloads

Basic Plus and Reserve. These terms differentiate the two ways Virtustream offers µVMs services.

"Basic Plus" µVM services are limited to a single Virtustream data center and have 99.99% availability for the Customer's committed level.

"Reserve" µVM services are an equivalent quantity of µVMs generally used for production workloads reserved at Customer-designated secondary Virtustream data center for on-going operation during disaster events and during scheduled disaster recovery (DR) exercises.

In both cases, overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

High Memory. Virtustream offers competitive pricing on compute services for applications that require large amounts of memory (64GiB or more) and high µVM consumption (32 µVMs and above).

Project Based. A few of the services listed are highly variable in scope and customer need. These services are billed as "project based." For these services, Virtustream will gather the scope and requirements to satisfy the need in a specific customer engagement, and the project will be scheduled and billed in accordance with those requirements.

Enterprise Zone. The "Enterprise" zone is for use by non-Internet facing workloads. Systems deployed into the Enterprise zone are not directly accessible from the Internet.

Additional terms can be found in Section 7, Definitions, starting on page 75.

2.1.2.1   Enterprise Basic Plus µVM (IC-uVM-BASP-ENT)

Enterprise Basic Plus µVMs reside in a single Virtustream data center, in the Enterprise zone. Resource availability is 99.99%, and only at the designated data center. Enterprise Basic Plus µVMs are used for non-Internet-accessible workloads.

Overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

Service Level. 99.99% availability for the Customer's committed level.

Billing. Monthly, based on resource usage.

Related
- *VPN Bandwidth*
- *Storage*

2.1.2.2   Enterprise Reserve µVM (IC-uVM-RESV-ENT)

Enterprise Reserve µVMs are generally used for production, non-Internet-accessible workloads. An equivalent quantity of µVMs that are used for production workloads are reserved at the Customer-designated secondary Virtustream data center for ongoing operation during disaster events and during scheduled disaster recovery (DR) exercises.

Overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

Service Level. N/A

Billing. Monthly, based on resource usage.

Related
- *VPN Bandwidth*
- *Storage - Local*
- *Storage - Replicated*

2.1.2.3   vHANA Installation and Setup Charge - Virtual Appliance (HM-HA-VIR-1T)

Setup and configuration of the Virtual HANA (vHANA) managed appliance. vHANA currently supports only the Scale-up HANA architecture.

Billing. One-time charge.

Required
- SUSE Linux Enterprise Server (SUSE) or Red Hat Enterprise Linux (RHEL) license (either Virtustream- or customer-provided)

2.1.2.4   High Memory Enterprise Basic VM Plus Fee (IC-HVM-BASP-ENT)

Applied to compute services for applications that require large amounts of memory (64GiB or more) and high µVM consumption (32 µVMs and above).

This surcharge is paired with the High Memory Enterprise Basic Plus µVM Fee, below.

Billing. Monthly, per VM.

Required
- *High Memory Enterprise Basic Plus µVM (IC-uHV-BASP-ENT)*

2.1.2.5   High Memory Enterprise Basic Plus µVM (IC-uHV-BASP-ENT)

Enterprise Basic Plus µVMs reside in a single Virtustream data center, in the Enterprise zone. The High Memory Enterprise Basic Plus µVM version is recommended for workloads in excess of 64GiBs of memory that are expected to consume 32 or more µVMs, and must be paired with a High Memory Enterprise Basic Plus VM Fee, above. Resource availability is 99.99%, and only at the designated data center. High Memory Enterprise Basic Plus µVMs are used for non-Internet-accessible workloads.

Overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

Service Level. 99.99% availability for the Customer's committed level.

Billing. Monthly, based on resource usage.

Related
- *VPN Bandwidth*
- *Storage - Local*

Required
- *High Memory Enterprise Basic Plus VM Fee (IC-HVM-BASP-ENT)*

2.1.2.6   High Memory Enterprise Reserve µVM (IC-uHV-RESV-ENT)

High Memery Enterprise Reserve µVMs are generally used for production, non-Internet-accessible workloads and recommended for workloads in excess of 64GiBs of memory. An equivalent quantity of µVMs generally used for production workloads are reserved at Customer designated secondary Virtustream data center for ongoing operation during disaster events and during scheduled disaster recovery (DR) exercises.

Overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level.

Service Level. N/A

Billing. Monthly, based on resource usage.

Related
- *VPN Bandwidth*
- *Storage - Local*
- *Storage - Replicated*

Required
- *High Memory Enterprise Core VM Fee (IC-HVM-COR-ENT)*

2.1.3   IaaS HANA Physical Appliances

Unlike other Virtustream services in this list, HANA physical appliances are not consumption based. Each is an individual hardware appliance, dedicated to an individual customer's use. HANA's high-performance, in-memory database operation is specifically designed to host SAP and other applications with demanding in-memory database requirements.

Virtustream provides the HANA appliances as hardware-only, allowing each customer to select the desired operating system based on their needs or preferences. Customers may provide their own OS licenses, or subscribe to either SUSE Linux Enterprise Server (SUSE or SLES) or Red Hat Enterprise Linux (RHEL) through Virtustream.

HANA appliances provided by Virtustream support either the HANA Scale-up architecture, or the HANA Scale-out architecture. The supported architecture is indicated in the product name as follows:

- "SOH/Standalone" indicates that the HANA appliance supports the HANA Scale-up architecture. This deployment architecture requires that all available capacity be present in a single HANA appliance. The only way to add capacity is to increase the resources within a given appliance, or to replace the current appliance with a system with more capacity. SAP ERP Central Component (ECC) is an example of an application that uses the HANA Scale-up architecture.

- "BW/Scale-out" indicates that the HANA appliance supports the HANA Scale-out architecture. This deployment architecture enables horizontal scalability. HANA capacity can be increased by adding

additional appliances (nodes) to a "cluster." SAP Business Warehouse (BW) is an example of an application that can use the HANA Scale-out architecture.

It is important to select the appliance type that is appropriate for the intended application needs.

2.1.3.1   HANA Appliance Installation and Setup - Physical Appliance (HM-HA-PHS 1T)

As setup and configuration of the Physical HANA managed appliance, Virtustream will perform the following:

- Procurement of Certified SAP HANA appliances or virtual HANA in an SAP Certified configuration (per contract)
- Install redundant power feeds to server cabinets
- Rack & Stack of HANA Appliances
- Implement cross connects between xStream Cloud and HANA Appliances
- Integrate existing Customer network for the new network requirements
- Install and configure SUSE or RHEL, per customer
- Install and configure the HANA DB environment
- Provide core HANA Database documentation information
- HANA Backup configuration and assistance
- Perform handover documentation review

The following is not part of the HANA Appliance Installation and Setup, but Virtustream may provide these services upon written request and written approval of Customer at the time and material rates set forth in the associated SOW:

- Install and configure the SAP environment along with the enhancement pack level, and patch level specified by Customer
- Document full SAP environment
- Install OS, SAP, and HANA monitoring and alerting configuration
- HANA DB Security Assistance

Billing. One-time charge, per appliance.

2.1.3.2   HANA Migration and Optimization (HM-HA-MIG-1T)

Migration and optimization of Customer's database into the HANA managed appliance.

Billing. One-time charge, project based.

2.1.3.3   6 TB HANA Managed Appliance for SOH - Primary (HM-HA1-SOH-6TB)

This is a single, dedicated physical HANA appliance with 6TiB of memory and 120 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *6 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-6TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.4   6 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-6TB)

This is a single, dedicated physical HANA appliance with 6TiB of memory and 120 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *6 TB HANA Managed Appliance for SOH - Primary (HM-HA1-SOH-6TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.5   3 TB HANA Managed Appliance for SOH - Primary (HM-HA1-SOH-3TB)

This is a single, dedicated physical HANA appliance with 3TiB of memory and 120 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *3 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-3TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.6   3 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-3TB)

This is a single, dedicated physical HANA appliance with 3TiB of memory and 120 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *3 TB HANA Managed Appliance for SOH - Primary (HM-HA1-SOH-3TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.7   2 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary (HM-HA1-SN-2TB)

This is a single, dedicated physical HANA appliance with 2TiB of memory and 80 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

If SAP "Suite on HANA" (SoH) is the single intended use for the HANA appliance, Virtustream offers an alternate, more cost effective SKU for that application: HM-HA1-SOH-2TB, 2 TB HANA Managed Appliance for SOH- Primary.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *2 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary (HM-HA2-SN-2TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*
- *2 TB HANA Managed Appliance for SOH- Primary (HM-HA1-SOH-2TB)*

2.1.3.8   2 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary (HM-HA2-SN-2TB)

This is a single, dedicated physical HANA appliance with 2TiB of memory and 80 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

If SAP "Suite on HANA" (SoH) is the single intended use for the HANA appliance, Virtustream offers an alternate, more cost effective SKU for that application: HM-HA2-SOH-2TB, 2 TB HANA Managed Appliance for SOH- Secondary.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *2 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary (HM-HA1-SN-2TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*
- *2 TB HANA Managed Appliance for SOH- Secondary (HM-HA2-SOH-2TB)*

2.1.3.9   2 TB HANA Managed Appliance for BW (Scale-Out) - Primary (HM-HA1-SO-2TB)

This is a single, dedicated physical HANA appliance with 2TiB of memory and 80 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP Business Warehouse" (BW) business intelligence software and other applications that support the HANA Scale-out architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *2 TB HANA Managed Appliance for BW (Scale-Out) - Secondary (HM-HA2-SO-2TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.10   2 TB HANA Managed Appliance for BW (Scale-Out) - Secondary (HM-HA2-SO-2TB)

This is a single, dedicated physical HANA appliance with 2TiB of memory and 80 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP Business Warehouse" (BW) business intelligence software and other applications that support the HANA Scale-out architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *2 TB HANA Managed Appliance for BW (Scale-Out) - Primary (HM-HA1-SO-2TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.11   2 TB HANA Managed Appliance for SOH - Primary (HM-HA1-SOH-2TB)

This is a single, dedicated physical HANA appliance with 2TiB of memory and 80 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *2 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-2TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.12   2 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-2TB)

This is a single, dedicated physical HANA appliance with 2TiB of memory and 80 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *2 TB HANA Managed Appliance for SOH- Primary (HM-HA1-SOH-2TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.13   1.5 TB HANA Managed Appliance for SOH - Primary (HM-HA1-SOH-15TB)

This is a single, dedicated physical HANA appliance with 1.5TiB of memory and 80 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1.5 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-15TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.14   1.5 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-15TB)

This is a single, dedicated physical HANA appliance with 1.5TiB of memory and 80 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1.5 TB HANA Managed Appliance for SOH- Primary (HM-HA1-SOH-15TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.15   1 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary (HM-HA1-SN-1TB)

This is a single, dedicated physical HANA appliance with 1TiB of memory and 80 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

If SAP "Suite on HANA" (SoH) is the single intended use for the HANA appliance, Virtustream offers an alternate, more cost effective SKU for that application: HM-HA1-SOH-1TB - 1 TB HANA Managed Appliance for SOH- Primary.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1 TB HANA Managed Appliance (Single Note/Scale-Up) - Secondary (HM-HA2-SN-1TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*
- *1 TB HANA Managed Appliance for SOH- Primary (HM-HA1-SOH-1TB)*

2.1.3.16 1 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary (HM-HA2-SN-1TB)

This is a single, dedicated physical HANA appliance with 1TiB of memory and 80 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

If SAP "Suite on HANA" (SoH) is the single intended use for the HANA appliance, Virtustream offers an alternate, more cost effective SKU for that application: HM-HA2-SOH-1TB - 1 TB HANA Managed Appliance for SOH- Secondary.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1 TB HANA Managed Appliance (Single Note/Scale-Up) - Primary (HM-HA1-SN-1TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*
- *1 TB HANA Managed Appliance for SOH- Secondary (HM-HA2-SOH-1TB)*

2.1.3.17 1 TB HANA Managed Appliance for BW (Scale-Out) - Primary (HM-HA1-SO-1TB)

This is a single, dedicated physical HANA appliance with 1TiB of memory and 80 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP Business Warehouse" (BW) business intelligence software and other applications that support the HANA Scale-out architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1 TB HANA Managed Appliance for BW (Scale-Out) - Secondary (HM-HA2-SO-1TB)*

- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.18   1 TB HANA Managed Appliance for BW (Scale-Out) - Secondary (HM-HA2-SO-1TB)

This is a single, dedicated physical HANA appliance with 2TiB of memory and 80 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP Business Warehouse" (BW) business intelligence software and other applications that support the HANA Scale-out architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1 TB HANA Managed Appliance for BW (Scale-Out) - Primary (HM-HA1-SO-1TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.19   1 TB HANA Managed Appliance for SOH - Primary (HM-HA1-SOH-1TB)

This is a single, dedicated physical HANA appliance with 1TiB of memory and 80 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-1TB)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.20   1 TB HANA Managed Appliance for SOH - Secondary (HM-HA2-SOH-1TB)

This is a single, dedicated physical HANA appliance with 1TiB of memory and 80 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *1 TB HANA Managed Appliance for SOH- Primary (HM-HA1-SOH-1TB)*

- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.21 512 GB HANA Managed Appliance (Single Node/Scale-Up) - Primary (HM-HA1-SN-512)

This is a single, dedicated physical HANA appliance with 512GiB of memory and 40 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *512 GB HANA Managed Appliance (Single Node/Scale-Up) - Secondary (HM-HA2-SN-512)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.22 512 GB HANA Managed Appliance (Single Node/Scale-Up) - Secondary (HM-HA2-SN-512)

This is a single, dedicated physical HANA appliance with 512GiB of memory and 40 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP "Suite on HANA" (SoH) and other applications that support the HANA Scale-up architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *512 GB HANA Managed Appliance (Single Node/Scale-Up) - Primary (HM-HA1-SN-512)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.23 512 GB HANA Managed Appliance BW (Scale-Out) - Primary (HM-HA1-SO-512)

This is a single, dedicated physical HANA appliance with 512GiB of memory and 40 CPU cores, and resides in Customer's Primary Virtustream data center.

It is certified for use with (but does not include) the SAP Business Warehouse" (BW) business intelligence software and other applications that support the HANA Scale-out architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *512 GB HANA Managed Appliance for BW (Scale-Out) - Secondary (HM-HA2-SO-512)*

- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.3.24 512 GB HANA Managed Appliance for BW (Scale-Out) - Secondary (HM-HA2-SO-512)

This is a single, dedicated physical HANA appliance with 512GiB of memory and 40 CPU cores, and resides in Customer's Secondary Virtustream data center.

It is certified for use with (but does not include) the SAP Business Warehouse" (BW) business intelligence software and other applications that support the HANA Scale-out architecture.

Service Level. 99.5% availability.

Billing. Customer's monthly fee provides individual use of the entire resource; there is no additional usage or overage charge.

Note: This item is hardware only. OS licenses can be provided by Customer, or purchased through Virtustream. Customer can bring SAP license.

Related
- *512 GB HANA Managed Appliance BW (Scale-Out) - Primary (HM-HA1-SO-512)*
- *SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)*
- *Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)*

2.1.4 OS, Database, and Other Software

2.1.4.1 Microsoft SQL Standard (per 2 cores) (IC-SW-MQL-STD)

Microsoft SQL Server, Standard Edition license for unlimited users per month (in accordance with applicable EULA attached in section 9.1).

Purchased in 2 core increments. Minimum is four cores; maximum 16 cores.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly fee based on the number of VM cores devoted to hosting the SQL server: one billing unit per every two cores with a minimum allocation of two billing units per VM.

2.1.4.2 Microsoft SQL Enterprise (per 2 cores) (IC-SW-MQL-ENT)

Microsoft SQL Server, Enterprise Edition license for unlimited users per month (in accordance with applicable EULA attached in section 9.1).

Purchased in 2 core increments. Minimum is 4 cores; maximum cores based on OS.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly fee based on the number of VM cores devoted to hosting the SQL server: one billing unit per every two cores with a minimum allocation of two billing units per VM.

2.1.4.3 SUSE Linux Enterprise ≤ 2 vCPU & ≤ 2GB RAM (IC-SW-SLES-2C)

SUSE Linux Enterprise Server (SLES) for x86, for use with VMs configured with not more than two virtual cores, not more than eight GiB RAM.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly subscription fee per hosted instance.

2.1.4.4 SUSE Linux Enterprise ≤ 4 vCPU & ≤ 8GB RAM (IC-SW-SLES-4C)

SUSE Linux Enterprise Server (SLES) for x86, for use with VMs configured with either three or four virtual cores, not more than eight GiB RAM.

Billing. Monthly subscription fee per hosted instance.

2.1.4.5   SUSE Linux Enterprise > 4 vCPU or > 8GB RAM (IC-SW-SLES-VM)

SUSE Linux Enterprise Server (SLES) for x86, for use with VMs configured with more than four virtual cores, and/or more than eight GiB RAM.

Billing. Monthly subscription fee per hosted instance.

2.1.4.6   SUSE Linux Enterprise for SAP ≤ 2 vCPU & ≤ 2GB RAM (IC-SW-SLES-S2C)

SUSE Linux Enterprise Server (SLES) for x86, for use with VMs configured with not more than two virtual cores, not more than eight GiB RAM. This version is optimized for use with SAP.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly subscription fee per hosted instance.

2.1.4.7   SUSE Linux Enterprise for SAP ≤ 4 vCPU & ≤ 8GB RAM (IC-SW-SLES-S4C)

SUSE Linux Enterprise Server (SLES) for x86, for use with VMs configured with either three or four virtual cores, not more than eight GiB RAM. This version is optimized for use with SAP.

Billing. Monthly subscription fee per hosted instance.

2.1.4.8   SUSE Linux Enterprise for SAP > 4 vCPU or >8GB RAM (IC-SW-SLES-SVM)

SUSE Linux Enterprise Server (SLES) for x86, for use with VMs (vCPUs) configured with more than four virtual cores, and/or more than eight GiB RAM. This version is optimized for use with SAP.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly subscription fee per hosted instance.

Related
- *Virtual HANA appliances*

2.1.4.9   SUSE Linux Enterprise for Physical HANA (IC-SW-SLES-PH)

SUSE Linux Enterprise Server (SLES) for x86, for use with physical HANA appliances.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly subscription fee per hosted instance.

Related
- *Physical HANA appliances*

2.1.4.10   Red Hat Enterprise Linux - Standard (per OS) (IC-SW-RHL-STD)

Red Hat Enterprise Linux (RHEL) for use with VMs configured with not more than four vCPUs.

If this product is included in the Services, Customer hereby assents and agrees to the Cloud Software Subscription Agreement (see Section 9.2) as of the Effective Date of this Service Description, and Customer acknowledges they have reviewed the text.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly subscription fee per hosted instance.

2.1.4.11   Red Hat Enterprise Linux - Enterprise (per OS) (IC-SW-RHL-ENT)

Red Hat Enterprise Linux (RHEL) for use with VMs configured with five or more vCPUs.

If this product is included in the Services, Customer hereby assents and agrees to the Cloud Software Subscription Agreement (see Section 9.2) as of the Effective Date of this SD and Customer acknowledges that they have reviewed the text. Usage is tracked and billed on an actual usage basis

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly subscription fee.

Related

- *Physical HANA appliances*
- *Virtual HANA appliances*

2.1.4.12 Microsoft OS (IC-SW-MSS-WIN)

Windows Server OS (in accordance with applicable EULA attached in section 9.1).

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly subscription fee, per instance.

2.1.4.13 Remote Desktop Services (per User) (IC-SW-RDS-IF)

Allows an end user to access a Microsoft Remote Desktop session host running on the Virtustream cloud platform.

Virtustream support is limited to license keys and downloads; software technical support is excluded.

Billing. Monthly per user.

2.1.5 IaaS Storage & Backup

2.1.5.1 Managed Backup Overview

Virtustream's Managed Backup Service is a fully managed service designed to facilitate restoration of data to the server from which the data originated in the event the primary data is lost or corrupted. Virtustream is responsible for all aspects of service delivery, including setup and configuration, ongoing management, 24x7 monitoring, restorations, and problem resolution.

The Managed Backup Service uses industry leading enterprise-class technologies (software and hardware) to backup protected data to disk-based systems which are located in Virtustream's secure data centers.

Primary and Secondary Data Centers. Each Virtustream customer's production workload is hosted in one of Virtustream's secure data centers; that data center is then referred to as the customer's Primary data center and local backups will reside on systems located within the Primary data center. If the customer chooses replicated system backup, the local backups will be configured to replicate to a second Virtustream data center in an alternate geographic location for offsite storage and recovery purposes; that data center is referred to as the customer's Secondary data center.

Billing is calculated monthly on a per GB of protected data basis. The calculated protected data amount takes into account several factors including overall amount of data on customer's production systems, the rate of change of that data, backup policies, and retention requirements. Restorations available for a fee.

Front End: Data that needs to be backed up

100 GB

5 Day retention, daily change rate of 5%

Protected: Amount nominally saved and restorable

100 GB	5GB	5GB	5GB	5GB	120 GB
Day 1	Day 2	Day 3	Day 4	Day 5	
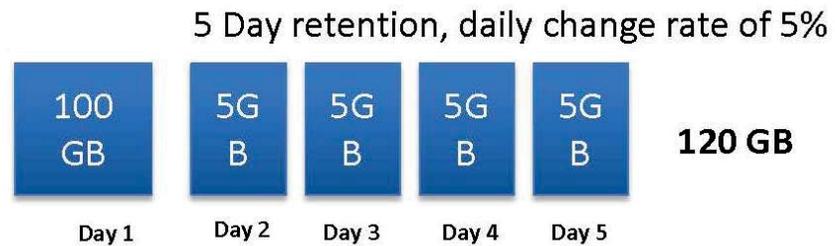
Backups and restorations from backups are intended to address use cases such as lost or deleted files, database corruption, viruses, and/or other types of system corruption. Restoration from backup is used when the production environment remains operational and there is a need to restore files, systems, or databases to a previous version. It is not intended to be used for recovering from a DR event.

Standard Virtustream backup policy is as follows:

- Production Storage: a full backup once weekly with daily incremental backups and a 30-day retention period
- Non-production Storage: full backup once weekly with daily incremental backups and 15-day retention period
- Custom backup policies and retention requirements will be considered on an individual customer basis

Both frequency and retention can vary based on individual customer contract and the total amount of protected data will vary accordingly. Increased retention and frequency will result in increased consumption.

Backup restoration is per VM to any of the retained save points. Restoration is a separate service and not included with the back-up service

Production VMs

**Backup Vault
Primary Data Center**

PRIVATE DC INTERCONNECTION

**Backup Vault
Secondary Data Center**
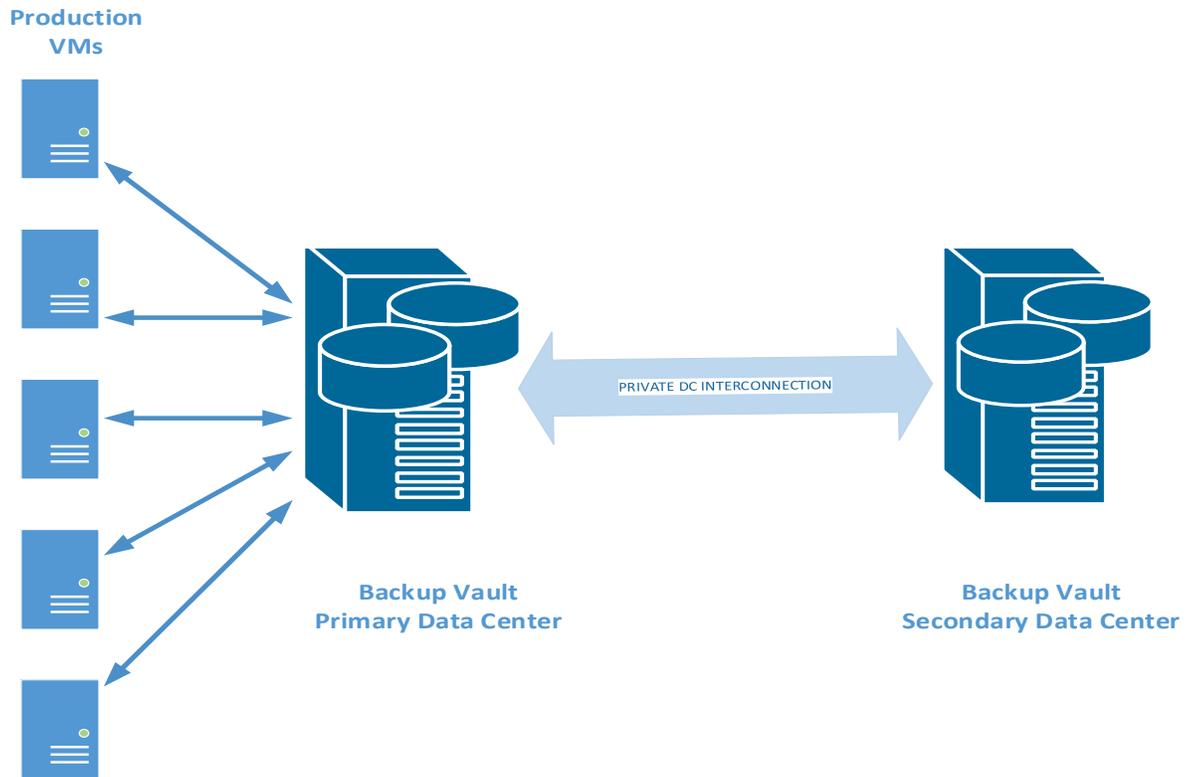
2.1.5.2   System Backup Setup (IC-DP-BU-1T)

One-time setup fee for setup and configuration of Customer's backup environment.

Billing. One-time charge, per account.

Related
- *System Backup - Replicated (IC-DP-BUP-REP)*
- *System Backup - Local Only (IC-DP-BUP-LOC)*

2.1.5.3   STANDARD System Backup (PROTECTED) - Replicated (IC-DP-BUP-REP)

This service provides file system backup at Customer's primary Virtustream data center. The backup is then replicated to Customer's secondary Virtustream data center.

Billing. Monthly fee per GB of protected data.

Required
- *System Backup Setup (IC-DP-BU-1T)*

Related
- *System Backup - Local Only (IC-DP-BU-LOC)*
- *Backup Restoration Request with CCS (IC-DP-BU-CRS)*
- *Backup Restoration Request without CCS (IC-DP-BU-NRS)*

2.1.5.4 STABDARD System Backup (PROTECTED)- Local Only (IC-DP-BUP-LOC)

This service provides file system backup at Customer's primary Virtustream data center only. Since there is no copy being replicated to a secondary site, this option will not provide back-up restoration when the primary data center is unavailable and should be chosen with this possibility in mind.

Billing. Monthly fee per GB of protected data.

Required
- *System Backup Setup (IC-DP-BU-1T)*

Related
- *System Backup - Replicated (IC-DP-BU-REP)*
- *Backup Restoration Request with CCS (IC-DP-BU-CRS)*
- *Backup Restoration Request without CCS (IC-DP-BU-NRS)*

2.1.5.5 HANA System Backup (Protected Data) - Replicated (IC-DP-BUPH-REP)

This service provides file system backup specifically for HANA at Customer's primary Virtustream data center. The backup is then replicated to Customer's secondary Virtustream data center.

Billing. Monthly fee per GB of protected data.

Required
- *System Backup Setup (IC-DP-BU-1T)*

Related
- *System Backup - Local Only (IC-DP-BU-LOC)*
- *Backup Restoration Request with CCS (IC-DP-BU-CRS)*
- *Backup Restoration Request without CCS (IC-DP-BU-NRS)*

2.1.5.6 HANA System Backup (Protected Data) - Local Only (IC-DP-BUPH-LOC)

This service provides file system backup for HANA at Customer's primary Virtustream data center only. Since there is no copy being replicated to a secondary site, this option will not provide back-up restoration when the primary data center is unavailable and should be chosen with this possibility in mind.

.

Billing. Monthly fee per GB of protected data.

Required
- *System Backup Setup (IC-DP-BU-1T)*

Related
- *System Backup - Replicated (IC-DP-BU-REP)*
- *Backup Restoration Request with CCS (IC-DP-BU-CRS)*
- *Backup Restoration Request without CCS (IC-DP-BU-NRS)*

2.1.5.7 Tier 0 Block Storage - Local Only (IC-STO-TOA-LOC)

Block storage with a Latency Service Level of 3ms that is maintained in a single data center with no replication capability.

Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

2.1.5.8   Tier I Block Storage - Local Only (IC-STO-T1A-LOC)

Block storage with a Latency Service Level of 10ms that is maintained in a single data center with no replication capability.

Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

2.1.5.9   Tier II Block Storage - Local Only (IC-STO-T2A-LOC)

Block storage with a Latency Service Level of 20ms that is maintained in a single data center with no replication capability.

Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

2.1.5.10   Tier III Block Storage - Local Only (IC-STO-T3A-LOC)

Block storage with a Latency Service Level Objective of 40ms that is maintained in a single data center with no replication capability.

Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.

2.1.5.11   Tier 0 Block Storage - Replicated (IC-STO-TOA-REP)

Data storage with a Latency Service Level of 3ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing. Monthly fee, based per GB of storage allocated.

2.1.5.12   Tier I Block Storage - Replicated (IC-STO-T1A-REP)

Data storage with a Latency Service Level of 10ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing. Monthly fee, based per GB of storage allocated.

2.1.5.13   Tier II Block Storage - Replicated (IC-STO-T2A-REP)

Data storage with a Latency Service Level of 20ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing. Monthly fee, based per GB of storage allocated.

2.1.5.14   Tier III Block Storage - Replicated (IC-STO-T3A-REP)

Data storage with a Latency Service Level Objective of 40ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes.

Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes.

Billing. Monthly fee, based per GB of storage allocated.

2.1.6   IaaS Network

2.1.6.1   Network Bandwidth Fee - USDC1 (IC-NW-BWU1-NET)

This Network Bandwidth service is for internet facing traffic in Virtustream's Washington, DC Data Center. Use of this Network Bandwidth provides public Internet access to systems in the DMZ. Enterprise zone connections are limited to outbound initiated connections through the firewall.

It does not provide direct access to systems in the Enterprise Zone. Likewise, Network Bandwidth does not provide direct access to the administrative interface of Customer's systems.

Internet Bandwidth requires a Virtustream Perimeter Firewall.

Network Bandwidth also supports the use of the Virtustream Load Balancer service (optional).

Billing. Network Bandwidth is billed monthly, at the 95th percentile of measured monthly Mbps usage, with no cap.

Required

- *Perimeter Firewall Configuration/Setup (CS-FW-FW-1T)*
- *Managed Perimeter Firewall (CS-FW-MPF-SVC)*

Related

- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

2.1.6.1   Network Bandwidth Fee - USDC2 (IC-NW-BWU2-NET)

This Network Bandwidth service is for internet facing traffic in Virtustream's San Francisco, CA Data Center. Use of this Network Bandwidth provides public Internet access to systems in the DMZ. Enterprise zone connections are limited to outbound initiated connections through the firewall.

It does not provide direct access to systems in the Enterprise Zone. Likewise, Network Bandwidth does not provide direct access to the administrative interface of Customer's systems.

Internet Bandwidth requires a Virtustream Perimeter Firewall.

Network Bandwidth also supports the use of the Virtustream Load Balancer service (optional).

Billing. Network Bandwidth is billed monthly, at the 95th percentile of measured monthly Mbps usage, with no cap.

Required

- *Perimeter Firewall Configuration/Setup (CS-FW-FW-1T)*
- *Managed Perimeter Firewall (CS-FW-MPF-SVC)*

Related

- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

2.1.6.2   Public IP Address (IPv6) (IC-NW-IPAD-V6)

A public IPv6 address allocated from the Virtustream address block.

Customer must provide DNS service.

Billing. Monthly fee per assigned public IPv6 IP address block.

2.1.6.3 Public IP Address (IPv4) (IC-NW-IPAD-V4)

A public IPv4 address allocated from the Virtustream address block.

Customer must provide DNS service.

Billing. Monthly fee per assigned public IPv4 IP address per month.

2.1.7 IaaS Load Balancer

2.1.7.1 Load Balancer Setup - Basic (IC-NW-LBB-1T)

In the case of customers who are comfortable defining their own load balancer requirements, Virtustream will provide a configuration template document to Customer for the definition of service list and rule preferences. Based on Customer's input, Virtustream will configure the load balancer.

Billing. One-time charge per load balancer configured by Virtustream.

Related
- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

2.1.7.2 Load Balancer Setup - Advanced (IC-NW-LBA-1T)

In the case of customers who need assistance in defining their load balancer requirements, Virtustream will engage with Customer in a two-hour technical session to define load balancer requirements. Virtustream will then design and configure the load balancer settings and iterate with Customer, as necessary.

Billing. One-time charge, per load balancer, and based on project scale determined during the technical session.

Related
- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

2.1.7.3 Load Balancing Bandwidth Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)

Charged in addition to network bandwidth per Mbps per month. Both managed load balancer service and network bandwidth are required.

Billing. Monthly fee per Mbps, based on the full Internet Bandwidth amount.

Required
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*
- *Network Bandwidth Fee - per Virtustream data center(s)*

2.1.7.4 Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)

Virtustream-managed load balancer service gives customers the ability to request changes to the load balancer configuration via the xOC (Virtustream's xStream Operations Center).

Billing. Monthly fee per VM in the DMZ.

Required
- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Network Bandwidth Fee - per Virtustream data center(s)*

2.1.8 IaaS Cloud & Storage Connect

Cloud Connect, USDC1 - Washington

2.1.8.1   Cloud Connect - Standard (24 ports available) - Setup - USDC1 (IC-NWU1-XCS-1T)

Installation of one 24-port, gigabit network switch in Virtustream's Washington, DC data center. Installation includes the necessary cabling to provide multiple Colo connections to the Virtustream cloud.

Related
- *Cloud Connect - Standard (24 ports available) - USDC1 (IC-NWU1-XCS-STD)*

2.1.8.2   Cloud Connect - Standard (24 ports available) - USDC1 (IC-NWU1-XCS-STD)

One managed, 24-port gigabit network switch in Virtustream's Washington, DC data center, providing connection from customer's environment on Virtustream IaaS Platform to colocated hardware, directly to Customers VRF environment.

Billing. Monthly fee is based on the number of managed cloud connect standard switches, and the number of managed firewalls.

Related
- *Network Bandwidth Fee - USDC1 (IC-NW-BWU1-NET)*
- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

2.1.8.3   Cloud Connect - HA (48 ports available) - Setup - USDC1 (IC-NWU1-XCH-1T)

Installation of two 24-port, gigabit network switches (for High Availability) in Virtustream's Washington, DC data center. Installation includes the necessary cabling, to provide multiple Colo HA connections to the Virtustream cloud.

Related
- *Cloud Connect - HA (48 ports available) - USDC1 (IC-NWU1-XCS-HA)*

2.1.8.4   Cloud Connect - HA (48 ports available) - USDC1 (IC-NWU1-XCS-HA)

Two managed, 24-port gigabit network switches (for a total of 48 ports) in Virtustream's Washington, DC data center, providing High Availability (HA) connection from customer's environment on Virtustream IaaS Platform to colocated hardware, directly to Customer's VRF environment.

Billing. Monthly fee is based on the number of managed cloud connect standard switches, and the number of managed firewalls.

Related
- *Network Bandwidth Fee - USDC1 (IC-NW-BWU1-NET)*
- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

Cloud Connect, USDC2 - San Francisco

2.1.8.5   Cloud Connect - Standard (24 ports available) - Setup - USDC2 (IC-NWU2-XCS-1T)

Installation of one 24-port, gigabit network switch in Virtustream's San Francisco, CA data center. Installation includes the necessary cabling to provide multiple Colo connections to the Virtustream cloud.

Related
- *Cloud Connect - Standard (24 ports available) - USDC2 (IC-NWU2-XCS-STD)*

2.1.8.6   Cloud Connect - Standard (24 ports available) - USDC2 (IC-NWU2-XCS-STD)

One managed, 24-port gigabit network switch in Virtustream's San Francisco, CA data center, providing connection from customer's environment on Virtustream IaaS Platform to colocated hardware, directly to Customers VRF environment.

Billing. Monthly fee is based on the number of managed cloud connect standard switches, and the number of managed firewalls.

Related
- *Network Bandwidth Fee - USDC2 (IC-NW-BWU2-NET)*
- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

2.1.8.7   Cloud Connect - HA (48 ports available) - Setup - USDC2 (IC-NWU2-XCH-1T)

Installation of two 24-port, gigabit network switches (for High Availability) in Virtustream's San Francisco, CA data center. Installation includes the necessary cabling, to provide multiple Colo HA connections to the Virtustream cloud.

Related
- *Cloud Connect - HA (48 ports available) - USDC2 (IC-NWU2-XCS-HA)*

2.1.8.8   Cloud Connect - HA (48 ports available) - USDC2 (IC-NWU2-XCS-HA)

Two managed, 24-port gigabit network switches (for a total of 48 ports) in Virtustream's San Francisco, CA data center, providing High Availability (HA) connection from customer's environment on Virtustream IaaS Platform to colocated hardware, directly to Customer's VRF environment.

Billing. Monthly fee is based on the number of managed cloud connect standard switches, and the number of managed firewalls.

Related
- *Network Bandwidth Fee - USDC2 (IC-NW-BWU2-NET)*
- *Load Balancing Fee (Additional to Network Bandwidth) (IC-NW-LBM-NET)*
- *Managed Load Balancer Services (per Server) (IC-NW-LBM-LB)*

Storage Connect, USDC1 - Washington

2.1.8.9   Storage Connect - Standard - Setup - USDC1 (IC-NWU1-SCS-1T)

Installation of one Fiber Channel switch in Virtustream's Washington, DC data center. Installation includes the necessary cabling.

Billing. One-time charge.

Related
- *Storage Connect - Standard - USDC1 (IC-NWU1-SCS-STD)*

2.1.8.10   Storage Connect - Standard - USDC1 (IC-NWU1-SCS-STD)

Single Fiber Channel switch providing Storage connectivity in Virtustream's Washington, DC data center.

Billing. Monthly fee, per switch.

2.1.8.11   Storage Connect - HA - Setup - USDC1 (IC-NWU1-SCH-1T)

Installation of two Fiber Channel switches in Virtustream's Washington, DC data center. Installation includes the necessary cabling.

Billing. One-time charge.

Related

- *Storage Connect - HA - USDC1 (IC-NWU1-SCS-HA)*

2.1.8.12   Storage Connect - HA - USDC1 (IC-NWU1-SCS-HA)

Dual Fiber Channel switches providing Storage connectivity in Virtustream's Washington, DC data center.

Billing. Monthly fee, per switch.

Storage Connect, USDC2 - San Francisco

2.1.8.13   Storage Connect - Standard - Setup - USDC2 (IC-NWU2-SCS-1T)

Installation of one Fiber Channel switch in Virtustream's San Francisco, CA data center. Installation includes the necessary cabling.

Billing. One-time charge.

Related

- *Storage Connect - Standard - USDC2 (IC-NWU2-SCS-STD)*

2.1.8.14   Storage Connect - Standard - USDC2 (IC-NWU2-SCS-STD)

Single Fiber Channel switch providing Storage connectivity in Virtustream's San Francisco, CA data center.

Billing. Monthly fee, per switch.

2.1.8.15   Storage Connect - HA - Setup - USDC2 (IC-NWU2-SCH-1T)

Installation of two Fiber Channel switches in Virtustream's San Francisco, CA data center. Installation includes the necessary cabling.

Billing. One-time charge.

Related

- *Storage Connect - HA - USDC2 (IC-NWU2-SCS-HA)*

2.1.8.16   Storage Connect - HA - USDC2 (IC-NWU2-SCS-HA)

Dual Fiber Channel switches providing Storage connectivity in Virtustream's San Francisco, CA data center.

Billing. Monthly fee, per switch.

2.1.9   IaaS Ad Hoc Services

2.1.9.1   DR Test Planning (IC-SVC-DR-PROJ)

Disaster Recovery (DR) Test Planning process produces Customer-specific DR Test Plan that specifies the scope of VMs, VLANs, and Storage (Data Stores) to be tested, is specific to the Customer environment, and can be conducted with minimal disruption to Customer's on-going production workload.

A Virtustream-verified DR Test Plan must be in place before any DR Test can be scheduled.

Note: DR Testing only applies to Core µVMs and replicated storage.

Billing. Per Project charge.

Related

- *DR Test Services - Tier 1 to 6*

2.1.9.2 DR Test Service - Tier 1 (10 VMs) (IC-SVC-DR1-AH)

Virtustream defines Disaster Recovery (DR) as the failover of processing from one hosting site to another in reaction to a data-center-wide emergency event. Tier 1 covers up to 10 VMs; one VLAN per five VMs; one Data Store per two VMs.

Virtustream's Disaster Recovery (DR) Test Service follows Customer's pre-existing DR Test Plan (see DR Test Planning, IC-SVC-DR-PROJ, above), and is comprised of three parts: Preparation, Failover, and Restoration. Virtustream will work collaboratively with the Customer throughout the test so as to minimize disruption to Customer's ongoing production workload.

RTO. 12 hours for complete failover to secondary data center.

Billing. One-time charge.

Related
- *DR Test Planning (IC-SVC-DR-PROJ)*

2.1.9.3 DR Test Service - Tier 2 (20 VMs) (IC-SVC-DR2-AH)

Virtustream defines Disaster Recovery (DR) as the failover of processing from one hosting site to another in reaction to a data-center-wide emergency event. Tier 2 covers up to 20 VMs; one VLAN per five VMs; one Data Store per two VMs.

Virtustream's Disaster Recovery (DR) Test Service follows Customer's pre-existing DR Test Plan (see DR Test Planning, IC-SVC-DR-PROJ, above), and is comprised of three parts: Preparation, Failover, and Restoration. Virtustream will work collaboratively with the Customer throughout the test so as to minimize disruption to Customer's ongoing production workload.

RTO. 12 hours for complete failover to secondary data center.

Billing. One-time charge.

Related
- *DR Test Planning (IC-SVC-DR-PROJ)*

2.1.9.4 DR Test Service - Tier 3 (40 VMs) (IC-SVC-DR3-AH)

Virtustream defines Disaster Recovery (DR) as the failover of processing from one hosting site to another in reaction to a data-center-wide emergency event. Tier 3 covers up to 40 VMs; one VLAN per five VMs; one Data Store per two VMs.

Virtustream's Disaster Recovery (DR) Test Service follows Customer's pre-existing DR Test Plan (see DR Test Planning, IC-SVC-DR-PROJ, above), and is comprised of three parts: Preparation, Failover, and Restoration. Virtustream will work collaboratively with the Customer throughout the test so as to minimize disruption to Customer's ongoing production workload.

RTO. 12 hours for complete failover to secondary data center.

Billing. One-time charge.

Related
- *DR Test Planning (IC-SVC-DR-PROJ)*

2.1.9.5 DR Test Service - Tier 4 (80 VMs) (IC-SVC-DR4-AH)

Virtustream defines Disaster Recovery (DR) as the failover of processing from one hosting site to another in reaction to a data-center-wide emergency event. Tier 4 covers up to 80 VMs; one VLAN per five VMs; one Data Store per two VMs.

Virtustream's Disaster Recovery (DR) Test Service follows Customer's pre-existing DR Test Plan (see DR Test Planning, IC-SVC-DR-PROJ, above), and is comprised of three parts: Preparation, Failover, and

Restoration. Virtustream will work collaboratively with the Customer throughout the test so as to minimize disruption to Customer's ongoing production workload.

RTO. 12 hours for complete failover to secondary data center.

Billing. One-time charge.

Related
- *DR Test Planning (IC-SVC-DR-PROJ)*

2.1.9.6   DR Test Service - Tier 5 (160 VMs) (IC-SVC-DR5-AH)

Virtustream defines Disaster Recovery (DR) as the failover of processing from one hosting site to another in reaction to a data-center-wide emergency event. Tier 5 covers up to 160 VMs; one VLAN per five VMs; one Data Store per two VMs.

Virtustream's Disaster Recovery (DR) Test Service follows Customer's pre-existing DR Test Plan (see DR Test Planning, IC-SVC-DR-PROJ, above), and is comprised of three parts: Preparation, Failover, and Restoration. Virtustream will work collaboratively with the Customer throughout the test so as to minimize disruption to Customer's ongoing production workload.

RTO. 18 hours for complete failover to secondary data center.

Billing. One-time charge.

Related
- *DR Test Planning (IC-SVC-DR-PROJ)*

2.1.9.7   DR Test Service - Tier 6 (320 VMs) (IC-SVC-DR6-AH)

Virtustream defines Disaster Recovery (DR) as the failover of processing from one hosting site to another in reaction to a data-center-wide emergency event. Tier 6 covers up to 320 VMs; one VLAN per five VMs; one Data Store per two VMs.

Virtustream's Disaster Recovery (DR) Test Service follows Customer's pre-existing DR Test Plan (see DR Test Planning, IC-SVC-DR-PROJ, above), and is comprised of three parts: Preparation, Failover, and Restoration. Virtustream will work collaboratively with the Customer throughout the test so as to minimize disruption to Customer's ongoing production workload.

RTO. 24 hours for complete failover to secondary data center.

Billing. One-time charge.

Related

2.1.9.8   Virtualization Right Sizing Report (IC-RPT-VRS-REQ)

The Right Sizing report is a recommendation of reconfiguration based on historical usage information.

Billing. Per report charge for a single custom period within the past six months.

2.1.9.9   Virtualization Custom Consumption Report (IC-RPT-VCC-REQ)

Custom consumption report for up to 500 VMs showing compute and storage utilization broken down by VM and resource pool.

Billing. Per report charge for a single custom period within the past 12 months.

2.1.9.10   Backup Restoration Request with CCS (IC-DP-BU-CRS)

Additional Backup Restorations beyond the included 10-per-month across the entire Customer estate (on a per-VM basis) — for customers with Cloud Cover Services.

Customers may also perform self-service backup restorations via a self-service interface.

Billing. Per backup restoration.

2.1.9.11 Backup Restoration Request without CCS (IC-DP-BU-NRS)

Additional Backup Restorations beyond the included 10-per-month across the entire Customer estate (on a per-VM basis) — for customers without Cloud Cover Services.

Customers may also perform self-service backup restorations via a self-service interface.

Billing. Per backup restoration.

2.2   Security Services: Network Based (Perimeter Defense)

2.2.1   Firewall

2.2.1.1   Firewall Configuration/Setup (CS-FW-FW-1T)

Virtustream firewall configuration and setup. Virtustream perimeter firewall services are required at each of Customer's Virtustream data center locations with Internet-facing bandwidth.

Billing. One-time charge per firewall.

Required
- *Network Bandwidth Fee - per Virtustream data center(s)*
- *Managed Perimeter Firewall (CS-FW-MPF-SVC)*

2.2.1.2   Managed Perimeter Firewall (CS-FW-MPF-SVC)

Virtustream-managed firewall service facilitates Customer firewall configuration change requests via the xOC (xStream Operations Center).

Billing. Monthly fee per VM in the DMZ.

Required
- *Firewall Configuration/Setup (CS-FW-FW-1T)*

2.2.2   IPSec VPN

2.2.2.1   IPSec VPN Host-Side Configuration (CS-VPN-H-1T)

IPSec VPN Tunnel configuration/management on Virtustream side at the Virtustream data center.

Billing. One-time charge, per VPN Tunnel.

Related
- *VPN Bandwidth Fee - per specific Virtustream data center*
- *IPSec VPN Client-Side Configuration (CS-VPN-C-1T)*

2.2.2.2   IPSec VPN Client-Side Configuration (CS-VPN-C-1T)

Remote support of customer's configuration of the IPSec VPN Tunnel at Customer site.

Billing. One-time charge, per VPN Tunnel.

Related
- *VPN Bandwidth Fee - per specific Virtustream data center*

2.2.2.3   IPSec VPN Bandwidth Fee - USDC1 (CS-VPN-U1-NET)

This IPSec VPN Bandwidth is intended for secure traffic via a site-to-site IPSec VPN connection between Customer's site and the Secure Landing Zone in Virtustream's data center in Washington, DC. It is not

for Internet facing traffic, and does not support user-to-site VPN connectivity. (See Network Bandwidth for internet-facing traffic.)

Billing. VPN Bandwidth is billed monthly, at the 95th percentile of measured monthly Mbps usage, with no cap.

Required
- *VPN Host-Side Configuration (CS-VPN-H-1T)*
- *VPN Client-Side Configuration (CS-VPN-C-1T)*

2.2.2.4   IPSec VPN Bandwidth Fee - USDC2 (CS-VPN-U2-NET)

This IPSec VPN Bandwidth is intended for secure traffic via a site-to-site IPSec VPN connection between Customer's site and the Secure Landing Zone in Virtustream's data center in San Francisco, CA. It is not for Internet facing traffic, and does not support user-to-site VPN connectivity. (See Network Bandwidth for internet-facing traffic.)

Billing. VPN Bandwidth is billed monthly, at the 95th percentile of measured monthly Mbps usage, with no cap.

Required
- *VPN Host-Side Configuration (CS-VPN-H-1T)*
- *VPN Client-Side Configuration (CS-VPN-C-1T)*

2.2.2.5   IPSec VPN Tunnel Managed Service Fee (CS-VPN-T-SVC)

Maintenance of circuit between Virtustream data center and Customer's facility.

Billing. Monthly, per VPN circuit.

2.2.3   Intrusion Detection Service (IDS) - Network-level

2.2.3.1   Network Based Intrusion Detection Primary Site Setup Charge (CS-IDS-NB1-1T)

Provides Intrusion Detection Services (IDS) installation and configuration at Customer's primary Virtustream data center.

Billing. One-time charge, per vLAN.

2.2.3.2   Network Based Intrusion Detection System and Managed Service Fee - Primary Site (CS-IDS-NB1-SYS)

This is a managed service for the network based Intrusion Detection Service (IDS) at Customer's primary Virtustream data center.

Virtustream will maintain the IDS rule set, auto-report generation, transmission of reports to Customer's defined recipients, load signatures each day, and develop daily, weekly, and monthly reports.

Frequency. The signature updates, online status, and operational health of the IDS system will be checked daily.

Billing. Monthly, per vLAN.

Required
- *Network Based Intrusion Detection Primary Site Setup Charge (CS-IDS-NB1-1T)*

2.2.3.3   Network Based Intrusion Detection Secondary Site Setup Charge (CS-IDS-NB2-1T)

Provides Intrusion Detection Services (IDS) installation and configuration at Customer's secondary Virtustream data center.

Billing. One-time charge, per vLAN.

2.2.3.4   Network Based Intrusion Detection System and Managed Service Fee - Secondary Site (CS-IDS-NB2-SYS)

This is a managed service for the network based Intrusion Detection Service (IDS) at Customer's secondary Virtustream data center.

Virtustream will maintain the IDS rule set, auto-report generation, transmission of reports to Customer's defined recipients, load signatures each day, and develop daily, weekly, and monthly reports.

Frequency. The signature updates, online status, and operational health of the IDS system will be checked daily.

Billing. Monthly, per vLAN.

Required
- *Network Based Intrusion Detection Secondary Site Setup Charge (CS-IDS-NB2-1T)*

2.3   Security Services: VM Level

2.3.1   Anti-Virus / Anti-Malware (AV/AM) - VM-level

2.3.1.1   Anti-Virus Primary System Setup (CS-TM-AV-1T)

Customer will fill out a specifications template, and Virtustream will deploy an anti-virus / anti-malware system to those specifications in Customer's primary Virtustream data center.

Note: Anti-Virus is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. One-time charge, per account.

Related
- *Anti-Virus Primary System fee (CS-TM-AV-SYS)*

2.3.1.2   Anti-Virus Primary System fee (CS-TM-AV-SYS)

Includes threat updates (multiple times per day), patches (multiple times per week), minor service pack releases, and major system upgrades for the AV / AM system at Customer's primary Virtustream data center.

Note: Anti-Virus is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly fee, per account.

Required
- *Anti-Virus Primary System Setup (CS-TM-AV-1T)*

2.3.1.3   Anti-Virus Secondary System Setup (CS-TM-AV-1T)

Customer will fill out a specifications template, and Virtustream will deploy an anti-virus / anti-malware system to those specifications in Customer's secondary Virtustream data center.

Note: Anti-Virus is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. One-time charge, per account.

Related
- *Anti-Virus Secondary System fee (CS-TM-AV-SYS)*

2.3.1.4 Anti-Virus Secondary System fee (CS-TM-AV-SYS)

Includes threat updates (multiple times per day), patches (multiple times per week), minor service pack releases, and major system upgrades for the AV / AM system at Customer's secondary Virtustream data center.

Note: Anti-Virus is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly fee, per account.

Required
- *Anti-Virus Secondary System Setup (CS-TM-AV-1T)*

2.3.1.5 Anti-Virus Managed Service Fee (CS-TM-AV1-SVC)

Virtustream manages and maintains the per-VM agents employed by the AV/AM system.

Note: Anti-Virus is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly fee, per VM.

2.3.2 Intrusion Detection Service (IDS) - VM-level

2.3.2.1 Intrusion Detection and Firewall Primary System Setup (CS-TM-IDFW-1T)

Setup of VM-level IDS and firewall monitoring & management system in Customer's primary Virtustream data center.

Note: IDS is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. One-time charge, per account.

2.3.2.2 Intrusion Detection and Firewall Primary System (CS-TM-IDFW-SYS)

Includes threat updates (multiple times per day), patches (multiple times per week), minor service pack releases, major system upgrades, and firewall rule changes for the IDS system at Customer's primary Virtustream data center.

Note: IDS is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly fee, per account.

Required
- *Intrusion Detection and Firewall Primary System Setup (CS-TM-IDFW-1T)*

2.3.2.3 Intrusion Detection and Firewall Secondary System Setup (CS-TM-IDFW-1T)

Setup of VM-level IDS and firewall in Customer's secondary Virtustream data center.

Note: IDS is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. One-time charge, per account.

2.3.2.4 Intrusion Detection and Firewall Secondary System (CS-TM-IDFW-SYS)

Includes threat updates (multiple times per day), patches (multiple times per week), minor service pack releases, major system upgrades, and firewall rule changes for the IDS system at Customer's secondary Virtustream data center.

Note: IDS is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly fee, per account.

Required
- *Intrusion Detection and Firewall Secondary System Setup (CS-TM-IDFW-1T)*

2.3.2.5   Intrusion Detection and Firewall Managed Service (CS-TM-IDFW1-SVC)

Virtustream manages all IDS and firewall rule change requests with normal service desk requests. Logs are stored for one year and are available upon request to client. IDS signatures are updated weekly.

Note: IDS is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly fee, per VM.

Related
- *Intrusion Detection and Firewall Primary System fee (CS-TM-IDFW-SYS)*
- *Intrusion Detection and Firewall Secondary System fee (CS-TM-IDFW-SYS)*

2.3.3   File Integrity Monitoring (FIM)

The File Integrity Manager (FIM) System monitors and detects changes to vital system elements, and delivers alerts and reports. System elements may include operating system files, installed software, running services, processes, directories, data files, file attributes, listening ports, registry keys, and registry values. Specific system elements to be monitored, as well as alerting and reporting parameters are defined by Customer during setup. In case of any compromise of these system elements, FIM can restore to a previously saved state.

2.3.3.1   File Integrity Monitoring Primary System Setup (CS-TM-FIM-1T)

Virtustream will install and configure a single instance of File Integrity Manager (FIM) in the Virtustream Cloud based on Customer specifications of alerting and reporting parameters delivered via a Virtustream-provided template.

Note: FIM is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. One time charge, per account.

Related
- *File Integrity Monitoring Primary System fee (CS-TM-FIM-SYS)*

2.3.3.2   File Integrity Monitoring Primary System (CS-TM-FIM-SYS)

Includes patches (multiple times per week), minor service pack releases, and major system upgrades for the FIM system at Customer's primary Virtustream data center.

File Integrity Manager System detects changes to vital system elements, as defined by the setup SKU, including operating system files, directories, data files, file attributes, and Windows Registry. In case of any compromise of these system elements, FIM can restore to a previous state.

Virtustream will maintain this system as hosted in the Virtustream cloud.

Note: FIM is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly, per account.

Required
- *File Integrity Monitoring Primary System Setup (CS-TM-FIM-1T)*

2.3.3.3   File Integrity Monitoring Secondary System Setup (CS-TM-FIM-1T)

Virtustream will work with Customer to define alerting and reporting parameters.

Virtustream will then install and configure a single instance of File Integrity Manager (FIM) in the Virtustream Cloud.

Note: Should be collocated with AV or other security server. If a dedicated VM is required (because of non-colocation for instance), there will be an additional cost.

Note: FIM is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. One time charge, per account.

Related
- *File Integrity Monitoring Secondary System fee (CS-TM-FIM-SYS)*

2.3.3.4   File Integrity Monitoring Secondary System (CS-TM-FIM-SYS)

Includes patches (multiple times per week), minor service pack releases, and major system upgrades for the FIM system at Customer's secondary Virtustream data center.

Note: FIM is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly, per account.

Required
- *File Integrity Monitoring Secondary System Setup (CS-TM-FIM-1T)*

2.3.3.5   File Integrity Monitoring Managed Service (CS-TM-FIM1-SVC)

Virtustream will monitor the FIM service, notify Customer when alerts are detected, and at Customer direction, restore to a previous state.

Note: FIM is also available as part of the VM-Level Security Bundle (VLSB), which provides three beneficial security services at a reduced bundle price.

Billing. Monthly Fee per VM.

Required
- *File Integrity Monitoring Primary System Setup (CS-TM-FIM-1T)*
- *File Integrity Monitoring Primary System fee (CS-TM-FIM-SYS)*

Related
- *File Integrity Monitoring Secondary System Setup (CS-TM-FIM-1T)*
- *File Integrity Monitoring Secondary System fee (CS-TM-FIM-SYS)*

2.3.4   VM-Level Security Bundle (VLSB)

The VM-Level Security Bundle (VSLB) is a suite of security services including the following:

- **Anti-Virus / Anti-Malware (AV/AM).** Includes threat updates, patches, and upgrades.
- **Firewall and Intrusion Detection Services (IDS).** Includes threat updates, patches, and upgrades, plus managed firewall rule change requests.
- **Integrity Monitoring (FIM).** A system that monitors and detects changes to vital system elements, and delivers alerts and reports.

2.3.4.1   VM-Level Security Bundle Primary System Setup (CS-TM-VLSB1-1T)

Customer will fill out a Virtustream-provided specifications template, and Virtustream will deploy a Customer-specific environment with a Customer-specific policy configuration in Customer's primary Virtustream data center. The environment setup will include a reporting console, report delivery setup, report cadence and distribution, configuration, and definition of protected hosts.

Billing. One-time, per account

2.3.4.2   VM-Level Security Bundle Primary System fee (CS-TM-VLSB1-SYS)

Includes threat updates (multiple times per day), patches (multiple times per week), minor service pack releases, major system upgrades, and firewall rule changes for the VLSB system at Customer's primary Virtustream data center.

Note: This bundle includes the services in the list, below.

Billing. Monthly fee, per VM.

Included
- *Anti-Virus Primary System (CS-TM-AV1-SYS)*
- *Anti-Virus Secondary System (CS-TM-AV2-SYS)*
- *Anti-Virus Managed Service (CS-TM-AV-SVC)*
- *File Integrity Monitoring Primary System (CS-TM-FIM1-SYS)*
- *File Integrity Monitoring Secondary System (CS-TM-FIM2-SYS)*
- *File Integrity Monitoring Managed Service (CS-TM-FIM-SVC)*
- *Intrusion Detection and Firewall Primary System (CS-TM-IDFW1-SYS)*
- *Intrusion Detection and Firewall Secondary System (CS-TM-IDFW2-SYS)*
- *Intrusion Detection and Firewall Managed Service (CS-TM-IDFW-SVC)*

2.3.4.3   VM-Level Security Bundle Secondary System Setup (CS-TM-VLSB2-1T)

Customer will fill out a Virtustream-provided specifications template, and Virtustream will deploy a Customer specific environment and with a customer-specific policy configuration in Customer's secondary Virtustream data center. The environment setup will include a reporting console, report delivery setup, report cadence and distribution, and definition of protected hosts.

Billing. One-time, per account.

2.3.4.4   VM-Level Security Bundle Secondary System fee (CS-TM-VLSB2-SYS)

Includes threat updates (multiple times per day), patches (multiple times per week), minor service pack releases, major system upgrades, and firewall rule changes for the VLSB system at Customer's secondary Virtustream data center.

Note: This bundle includes the services in the list, below.

Billing. Monthly fee, per account.

Included
- *Anti-Virus Primary System (CS-TM-AV1-SYS)*
- *Anti-Virus Secondary System (CS-TM-AV2-SYS)*
- *Anti-Virus Managed Service (CS-TM-AV-SVC)*
- *File Integrity Monitoring Primary System (CS-TM-FIM1-SYS)*
- *File Integrity Monitoring Secondary System (CS-TM-FIM2-SYS)*
- *File Integrity Monitoring Managed Service (CS-TM-FIM-SVC)*
- *Intrusion Detection and Firewall Primary System (CS-TM-IDFW1-SYS)*
- *Intrusion Detection and Firewall Secondary System (CS-TM-IDFW2-SYS)*
- *Intrusion Detection and Firewall Managed Service (CS-TM-IDFW-SVC)*

2.3.4.5   VM-Level Security Bundle Service Fee (<101 VMs) (CS-TM-VLSBA-SVC)

Ongoing monitoring of Customer VLSB system, including report delivery and distribution, and monitoring of protected hosts.

Billing. Monthly fee, per VM, for environments with fewer than 101 VMs.

2.3.4.6   VM-Level Security Bundle Service Fee (<1,001 VMs) (CS-TM-VLSBB-SVC)

Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.

Billing. Monthly fee, per VM, for environments with fewer than 1,001 VMs.

2.3.4.7   VM-Level Security Bundle Service Fee (<10,001 VMs) (CS-TM-VLSBC-SVC)

Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.

Billing. Monthly fee, per VM, for environments with fewer than 10,001 VMs.

2.3.4.8   VM-Level Security Bundle Service Fee (>10,000 VMs) (CS-TM-VLSBD-SVC)

Ongoing monitoring of Customer environment, including report delivery and distribution, and monitoring of protected hosts.

Billing. Monthly fee, per VM, for environments with more than 10,000 VMs.

2.3.5   Encryption

2.3.5.1   Encryption Management System Setup - SaaS (CS-ENC-SYSS-1T)

Configuration of Customer in shared encryption system to manage encryption agents.

Billing. One-time charge, per account.

Related
- *Encryption System Fee (CS-ENC-SYS-SYS)*

2.3.5.2   Encryption Management System Setup - Dedicated (CS-ENC-SYSD-1T)

Setup and configuration of a Customer-specific, dedicated encryption system to manage encryption agents.

Billing. One-time charge, per account.

Related
- *Encryption System Fee (CS-ENC-SYS-SYS)*

2.3.5.3   Encryption Management System Fee (CS-ENC-SYS-SYS)

Virtustream will monitor the operation of the encryption service and monitor for exceptions.

Billing is monthly, per system.

Required
- *Encryption System Setup(CS-ENC-SYSS-1T)*

plus one or more of the following
- *Encryption Agent Fee (Non-Production) (CS-ENC-AGT-NP)*
- *Encryption Agent Fee (Production) (CS-ENC-AGT-PR)*
- *HANA Encryption Agent Fee (Non-Production) (CS-ENC-AGTH-NP)*
- *HANA Encryption Agent Fee (Production) (CS-ENC-AGTH-PR)*

2.3.5.4 Encryption Agent Setup (CS-ENC-AGT-1T)

Setup for each of encryption agent for each protected VM.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing. One-time charge, per protected VM.

Related
- *Encryption Agent Fee (Non-Production) (CS-ENC-AGT-NP)*
- *Encryption Agent Fee (Production) (CS-ENC-AGT-PR)*

2.3.5.5 Encryption Production Agent per vCPU Fee (CS-ENC-AGTC-PR)

This fee covers agents in Customer's production environment.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per vCPU, per system on which agent is installed.

Required
- *Encryption Agent Setup (CS-ENC-AGT-1T)*

2.3.5.6 Encryption Non-Production Agent per vCPU Fee (CS-ENC-AGTC-NP)

This fee covers agents in Customer's non-production environment.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per vCPU, per system on which agent is installed.

Required
- *Encryption Agent Setup (CS-ENC-AGT-1T)*

2.3.5.7 HANA Encryption Agent Setup (CS-ENC-AGTH-1T)

Setup the encryption agent on a HANA appliance (physical or virtual).

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing. One-time charge, per protected HANA appliance.

Related
- *HANA Encryption Agent Fee (Non-Production) (CS-ENC-AGTH-NP)*
- *HANA Encryption Agent Fee (Production) (CS-ENC-AGTH-PR)*

2.3.5.8 HANA Encryption Agent Fee (Production) (CS-ENC-AGTH-PR)

This fee covers agents on HANA appliances in Customer's production environment.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per HANA appliance, per 16 vCPUs.

Required
- *HANA Encryption Agent Setup (CS-ENC-AGTH-1T)*

2.3.5.9 HANA Encryption Agent Fee (Non-Production) (CS-ENC-AGTH-NP)

This fee covers agents on HANA appliances in Customer's non-production environment.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per 16 vCPUs.

Required
- *HANA Encryption Agent Setup (CS-ENC-AGTH-1T)*

2.3.5.10 High Memory Encryption Agent Setup (CS-ENC-AGTM-1T)

Setup for each of encryption agent for each High Memory VM.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing. One-time charge, per VM.

Related
- *High Memory Encryption Agent Fee (Non-Production) (CS-ENC-AGTM-NP)*
- *High Memory Encryption Agent Fee (Production) (CS-ENC-AGTM-PR)*

2.3.5.11 High Memory Encryption Agent Fee (Production) (CS-ENC-AGTM-PR)

This fee covers agents on High Memory VMs in Customer's production environment.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per vCPU, per system on which agent is installed.

Required
- *High Memory Encryption Agent Setup (CS-ENC-AGTM-1T)*

2.3.5.12 High Memory Encryption Agent Fee (Non-Production) (CS-ENC-AGTM-NP)

This fee covers agents on High Memory VMs in Customer's non-production environment.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per vCPU, per system on which agent is installed.

Required
- *High Memory Encryption Agent Setup (CS-ENC-AGTM-1T)*

2.3.5.13 Encryption Production Agent per VM Fee (CS-ENC-AGTV-PR)

Description.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per VM.

2.3.5.14 Encryption Non-Production Agent per VM Fee (CS-ENC-AGTV-NP)

Description.

"Agents" are the software that resides on each system that requires encryption capabilities. Agents enforce the encryption policy as defined in the encryption management system.

Billing is monthly, per VM.

2.3.6   Vulnerability Scanning

2.3.6.1   Vulnerability Scanning Managed Service - non Public IP (CS-VS-NPIP-SVC)

This service scans non-public IP endpoints within the customer's Virtustream environment and generates reports on possible network vulnerabilities based on recognized signatures. Virtustream security personnel will help the customer understand and prioritize any issues found by the scan.

The service includes:

- Authenticated OS level scanning and network vulnerability discovery
- Up-to-date vulnerability signature detections
- Monthly report delivery with recommended prioritization for remediation
- Monthly 30-minute readout of findings with Virtustream security personnel

Billing. Monthly, per public IP address.

2.3.6.2   Vulnerability Scanning Managed Service - Public IP (CS-VS-PIP-SVC)

This service scans public IP endpoints within the customer's Virtustream environment and generates reports on possible network vulnerabilities based on recognized signatures. Virtustream security personnel will help the customer understand and prioritize any issues found by the scan.

The service includes:

- Authenticated OS level scanning and network vulnerability discovery
- Up-to-date vulnerability signature detections
- Monthly report delivery with recommended prioritization for remediation
- Monthly 30-minute readout of findings with Virtustream security personnel

Billing. Monthly, per public IP address.

2.3.7   Distributed Denial of Service (DDoS) Monitoring

2.3.7.1   DDoS Monitoring and Reporting (5 Public IP Addresses) - Setup (CS-DDOS-MR-1T)

Distributed Denial of Service (DDoS) monitoring and reporting setup and configuration.

Billing. One-time charge, per five (5) Public IP addresses.

2.3.7.2   DDoS Monitoring and Reporting (5 Public IP Addresses) (CS-DDOS-MR-SVC)

Distributed Denial of Service monitoring and reporting, consisting of ongoing alert and monthly reporting on statistics for traffic to and from the IP address, for up to five (5) public IP addresses.

Billing. Monthly fee, per five (5) Public IP addresses.

2.3.8   Log Management

2.3.8.1   Log Management System Setup (CS-V-LM-1T)

Installation and configuration of the log management system.

Billing. One-time charge, per system.

Related
- *Log Management System Fee (CS-VC-LM-SYS)*

2.3.8.2   Managed Log Management Service Setup (CS-VS-MLM-1T)

Configuration of the Log Management System per the log management requirements.

Billing. One-time charge, per VM.

Related
- *Managed Log Management Service Fee (CS-VS-MLM-SVC)*

2.3.8.3   Log Management System Fee (CS-VC-LM-SYS)

Fee for the log aggregation system, which provides up to 5 GB total aggregate log volume per day for all VMs.

Billing. Monthly Fee, per system.

Required
- *Log Management System Setup (CS-V-LM-1T)*

2.3.8.4   Managed Log Management Service (CS-VS-MLM-SVC)

Fee for the log aggregation service.

Note: The service has a 5GB upper limit for the total aggregate log volume per day for all managed VMs. Logging will work if volume exceeds license (a "violation"), but searching will not. Five (5) license violations allowed per month. Virtustream will monitor and advise when additional log capacity licenses or tuning of logging devices will be necessary.

Billing. Monthly Fee, per VM.

Required
- *Managed Log Management Service Setup (CS-VS-MLM-1T)*

2.3.9   Security Policy Audit Services

2.3.9.1   Firewall Audit System Setup (CS-VS-FA-1T)

Virtustream installation and configuration of the Firewall Audit Management System.

Note: Should be collocated with AV or other security server. If a dedicated VM is required (because of non-colocation for instance), there will be an additional cost.

Billing. One-time charge.

Related
- *Firewall Audit System Fee (CS-VS-FA-SYS)*

2.3.9.2   Firewall Audit Export Setup (CS-VS-FAE-1T)

Virtustream will configure Customer designated firewall in the Virtustream cloud to export its settings to the Firewall Audit Manager, and then test to verify the configuration.

Billing. One-time charge, per firewall, per configuration request.

Related
- *Firewall Audit System Fee (CS-VS-FA-SYS)*

2.3.9.3   Firewall Audit System (CS-VS-FA-SYS)

Virtustream will maintain the Firewall Audit system, which monitors changes to the network security policy and maintains a complete audit trail.

Billing. Monthly, per system.

Required
- *Firewall Audit System Setup (CS-VS-FA-1T)*

2.3.9.4 Managed Firewall Auditing Service (CS-VS-MFA-SVC)

Virtustream will export the data from managed firewalls on a monthly basis and perform analysis of supported firewalls as a scheduled audit. The resulting reports will be reviewed by Virtustream security analysts and reviewed with Customer, as necessary.

Billing. Monthly, per managed firewall.

Required
- *Firewall Audit System Setup (CS-VS-FA-1T)*
- *Firewall Audit Export Setup (CS-VS-FAE-1T)*

2.3.9.5 Policy Auditor System Setup (CS-VS-PSYS-1T)

For customers who want a dedicated Firewall Policy Audit (FWPA) system, this service includes the tasks necessary to install a dedicated FWPA system within the Customer's environment.

Billing. One-time charge, per System.

Related
- *Policy Auditor System Fee (CS-VS-PA-SYS)*

2.3.9.6 Policy Auditor Service Setup (CS-VS-PSVC-1T)

This service includes the tasks required to configure a customer in either the Shared Firewall Policy Auditing System or a Dedicated Policy Auditor System.

Billing. One-time charge, per VM.

Required - one of the following
- *Access to Shared Firewall Policy Auditing System, or*
- *Dedicated Policy Auditor System Setup (CS-VS-PSYS-1T)*

2.3.9.7 Policy Auditor System Fee (CS-VS-PA-SYS)

Virtustream will provide a Policy Auditor system that is dedicated for use by a single customer. No components of the system are shared with other Virtustream tenants. The service includes patches, minor service pack releases, and major system upgrades for the customer's dedicated Policy Auditor system.

Billing. Monthly, per System.

Required
- *Policy Auditor System Setup (CS-VS-PSYS-1T)*

2.3.9.8 Policy Auditor Service Fee (CS-VS-PA-SVC)

Fee for the performance of the firewall policy analysis. Deliverables include: Risky Rule report, Rule Optimization Report, PCI Compliance Report. Reports are reviewed by certified Security Analysts and false positives are removed. Reports are delivered encrypted and passwords are delivered via out of band secure password exchange method. Expert comments and observations are attached to the report.

Billing. Recurring periodic, based on audits-per-year selected by customer: monthly (x12), quarterly (x4), semi-annually (x2), or annually (x1).

Required
- *Policy Auditor Service Setup (CS-VS-PSVC-1T)*

2.3.10   Two-Factor Authentication (2FA)

2.3.10.1   2FA Virtustream Portal Token Issue (CS-2F-VPT-1T)

Virtustream will register a 2FA token for the Virtustream Portal, and provide users with information and, when necessary, training for how to use tokens. Once the token is issued, Customer can recycle the tokens by reassigning the token to a different user or device, or Customer's own dedicated 2FA management system.

Billing. One-time charge when the token is issued (enrolled). (Note: Customer gets 2 tokens for free.)

Related
- *2FA Virtustream Portal Token Fee (CS-2F-VPT-MF)*

2.3.10.2   2FA Virtustream Portal Token Fee (CS-2F-VPT-MF)

Fee for ongoing use of each 2FA token for the Virtustream Portal.

Billing. Monthly fee for tokens used to access the Virtustream portal. (Note: Customer gets 2 tokens for free.)

Required
- *2FA Virtustream Portal Token Issue (CS-2F-VPT-1T)*

2.3.10.3   2FA Dedicated Setup (CS-2F-D1-1T)

Virtustream will install and configure a single instance of 2FA management system on a per Tenant basis. "Tenant" is defined as a single Active Directory (AD) domain. Virtustream will supply Customer with information required to integrate to Customer's designated Active Directory, with up to 4 hours of support. Virtustream will set up and configure a Windows OS VM in the Virtustream cloud and install the 2FA Management System. Virtustream will provide up to three hours of web based training to Customer designated administrators of the 2FA Management System.

Billing. One-time charge, per instance.

Related
- *2FA Dedicated Base Fee (CS-2F-D1-SYS)*
- *2FA Dedicated DR Setup (CS-2F-D2-1T)*

2.3.10.4   2FA Dedicated Self-Service Setup (CS-2F-DS-1T)

Customer will install and configure a single instance of the 2FA Management System on a per Tenant basis. "Tenant" is defined as a single Active Directory (AD) domain. Virtustream will supply Customer with information required to integrate to Customer's designated Active Directory. Customer will use the information provided to set up and configure Windows OS VM in the Virtustream cloud and install the 2FA Management System.

Billing. One-time charge, per instance.

Related
- *2FA Dedicated Base Fee (CS-2F-D1-SYS)*
- *2FA Dedicated DR Setup (CS-2F-D2-1T)*

2.3.10.5   2FA Dedicated Base Fee (CS-2F-D1-SYS)

This is a monthly fee for a single instance of a Customer's dedicated 2FA Management System at Customer's primary Virtustream data center.

The fee includes five (5) tokens licensed for one (1) year. Virtustream will implement the 2FA Management System software updates as issued by the manufacturer. Virtustream will implement one (1) update per year to the 2FA Management System if Customer Active Directory is upgraded or

changed. Any additional updates to the 2FA Management System as a result of Customer actions must be procured through Virtustream professional services. Virtustream will provide 24x7 help desk support for any tier 2 support issues.

Billing. Monthly fee per dedicated 2FA Management System.

Required - one of the following
- *2FA Dedicated Setup (CS-2F-D1-1T)*
- *2FA Dedicated Self-Service Setup (CS-2F-DS-1T)*

2.3.10.6 2FA Dedicated DR Setup (CS-2F-D2-1T)

Virtustream will install and configure a single instance of the 2FA Management System on a per Tenant basis in Customer's secondary Virtustream data center. "Tenant" is defined as a single Active Directory (AD) domain. Virtustream will supply Customer with information required to integrate to Customer's designated Active Directory, with up to one hour of support. Virtustream will set up and configure Windows OS VM in the Virtustream cloud and install the 2FA Management System.

Billing. One-time charge, per single instance of Customer's DR 2FA Management System.

Related
- *2FA Dedicated DR Base Fee (CS-2F-D2-SYS)*

2.3.10.7 2FA Dedicated DR Base Fee (CS-2F-D2-SYS)

This is a monthly fee for a single instance of a Customer's dedicated 2FA Management System at Customer's secondary Virtustream data center.

The fee includes five (5) tokens licensed for one year. Virtustream will implement the 2FA Management System software updates as issued by the manufacturer. Virtustream will implement one update per year to the 2FA Management System if Customer Active Directory (AD) is upgraded or changed. Any additional updates to the 2FA Management System as a result of Customer actions must be procured through Virtustream professional services. Virtustream will provide 24x7 help desk support for any tier 2 support issues.

Billing. Monthly fee per dedicated 2FA Management System.

Required
- *2FA Dedicated DR Setup (CS-2F-D2-1T)*

2.3.10.8 2FA Dedicated Token Issue (CS-2F-DT-1T)

Customer personnel will issue and install a 2FA token on a mobile device or computer. Virtustream will provide 24x7 help desk for any tier 2 support issues encountered during token registration. Once the token is issued, Customer can recycle the tokens by reassigning the token to a different user or device, or the Virtustream Portal.

Billing. One-time charge per 2FA token. (Note: Customer gets 2 tokens for free.)

Related
- *2FA Dedicated Token Fee (CS-2F-DT-MF)*

2.3.10.9 2FA Dedicated Token Fee (CS-2F-DT-MF)

This is a monthly fee for the use of 2FA Tokens associated with the 2FA Management System, for both the Virtustream Portal and Customer's own dedicated 2FA Management System.

This service includes a 3-year license for the 2FA Management System and one 2FAtoken. Virtustream will provide 24x7 help desk support for any tier 2 support issues.

Billing. Monthly fee based on the number of tokens issued and managed by the 2FA Management System.

Required
- *2FA Dedicated Token Issue (CS-2F-DT-1T)*

2.3.10.10 2FA Shared Setup (CS-2F-S-1T)

Virtustream will assist Customer in setting up an account in Virtustream's Shared 2FA Management System. Virtustream will supply Customer with information required to integrate to Customer's designated Active Directory (AD), with up to 4 hours of support. Virtustream will provide up to three hours of web based training to Customer designated administrators of the shared 2FA management account.

Billing. One-time charge, per shared 2FA Management account setup.

Related
- *2FA Shared Token Fee (CS-2F-ST-MF)*

2.3.10.11 2FA Shared Self-Service Setup (CS-2F-SS-1T)

Customer will set up an account in Virtustream's Shared 2FA Management System. Virtustream will supply Customer with information required to integrate to Customer's designated Active Directory (AD).

Billing. One-time charge, per shared 2FA Management account setup.

Related
- *2FA Shared Token Fee (CS-2F-ST-MF)*

2.3.10.12 2FA Shared Token Issue (CS-2F-ST-1T)

Customer personnel will issue and install a 2FA token on a mobile device or computer. Virtustream will provide 24x7 help desk for any tier 2 support issues encountered during token registration. Once the token is issued, Customer can recycle the tokens by reassigning the token to a different user or device, or the Virtustream Portal.

Billing. One-time charge per 2FA token. (Note: Customer gets 2 tokens for free.)

Required - one of the following
- *2FA Shared Setup (CS-2F-S-1T)*
- *2FA Shared Self-Service Setup (CS-2F-SS-1T)*

2.3.10.13 2FA Shared Token Fee (CS-2F-ST-MF)

This is a monthly fee for the use of 2FA Tokens associated with the 2FA Management System, for both the Virtustream Portal and an account in Virtustream's Shared 2FA Management System.

This service includes a 3-year license for the 2FA Management System and one 2FAtoken. Virtustream will provide 24x7 help desk support for any tier 2 support issues.

Billing. Monthly fee based on the number of tokens issued and managed by the 2FA Management System.

Required
- *2FA Shared Token Issue (CS-2F-ST-1T)*

2.4.1.1   Fiber Cross Connect - Vienna - Installation (DC-NWU1-XCF-1T)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The fiber version of Cross Connect provides both higher bandwidth and greater transmission distance than the copper version.

Installation Time (typical). Five to eight business days; varies based on the distance between connection points.

Bandwidth. Up to 10Gbs.

Transmission Distance. Virtually unlimited within the data center.

Billing. One-time charge per cross connect.

2.4.1.2   Fiber Cross Connect - Vienna (DC-NWU1-XCF-MF)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The fiber version of Cross Connect provides both higher bandwidth and greater transmission distance than the copper version.

Bandwidth. Up to 10Gbs.

Billing. Monthly, per cross connect.

Required
- *Fiber Cross Connect - Vienna - Installation (DC-NWU1-XCF-1T)*

2.4.1.3   Copper Cross Connect - Vienna - Installation (DC-NWU1-XCC-1T)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The copper version of Cross Connect is both lower bandwidth and capable of a shorter transmission distance than the fiber version — but at a lower cost.

Installation Time (typical). Five to eight business days; varies based on the distance between connection points.

Bandwidth. Up to 1Gbs.

Transmission Distance. Up to 300 feet within the data center. Note that, because of wiring channel locations and other factors, the wiring distance between data center racks may be substantially longer than a simple straight line.

Billing. One-time charge per instance.

2.4.1.4   Copper Cross Connect - Vienna (DC-NWU1-XCC-MF)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The copper version of Cross Connect is both lower bandwidth and capable of a shorter transmission distance than the fiber version — but at a lower cost.

Bandwidth. Up to 1Gbs.

Billing. Monthly, per cross connect.

Required
- *Copper Cross Connect - Vienna - Installation (DC-NWU1-XCC-1T)*

2.4.1.5   Hotel Rack (1U) - Managed Colo - Vienna (DC-RKU1-RK-HR)

This service provides Customer with one (1) rack unit (RU) in a shared rack within a Virtustream data center. Included with this service are 2x 1G Copper interfaces.

Billing. Monthly, per 1U slot.

Required, one of the following:

- *Remote Eyes & Hands (US) - Bronze (DC-SVC-REU-B)*
- *Remote Eyes & Hands (US) - Silver (DC-SVC-REU-S)*
- *Remote Eyes & Hands (US) - Gold (DC-SVC-REU-G)*

2.4.2   US Data Center 2 (San Francisco)

2.4.2.1   Fiber Cross Connect - San Francisco - Installation (DC-NWU2-XCF-1T)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The fiber version of Cross Connect provides both higher bandwidth and greater transmission distance than the copper version.

Installation Time (typical). Five to eight business days; varies based the distance between connection points.

Bandwidth. Up to 10Gbs.

Transmission Distance. Virtually unlimited within the data center.

Billing. One-time charge per cross connect.

2.4.2.2   Fiber Cross Connect - San Francisco (DC-NWU2-XCF-MF)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The fiber version of Cross Connect provides both higher bandwidth and greater transmission distance than the copper version.

Installation Time (typical). Five to eight business days; varies based on the distance between connection points.

Bandwidth. Up to 10Gbs.

Transmission Distance. Virtually unlimited within the data center.

Billing. Monthly, per cross connect.

Required
- *Fiber Cross Connect - San Francisco - Installation (DC-NWU2-XCF-1T)*

2.4.2.3   Copper Cross Connect - San Francisco - Installation (DC-NWU2-XCC-1T)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The copper version of Cross Connect is both lower bandwidth and capable of a shorter transmission distance than the fiber version — but at a lower cost.

Installation Time (typical). Five to eight business days; varies based on the distance between connection points.

Bandwidth. Up to 1Gbs.

Transmission Distance. Up to 300 feet within the data center. Note that, because of wiring channel locations and other factors, the wiring distance between data center racks may be substantially longer than a simple straight line.

Billing. One-time charge per cross connect.

2.4.2.4   Copper Cross Connect - San Francisco (DC-NWU2-XCC-MF)

Cross Connect is necessary to provide a connection between a customer's rack-installed colocated equipment and Customer's other Virtustream provided, cloud-based services in the data center.

The copper version of Cross Connect is both lower bandwidth and capable of a shorter transmission distance than the fiber version — but at a lower cost.

Installation Time (typical). Five to eight business days; varies based on the distance between connection points.

Bandwidth. Up to 1Gbs.

Transmission Distance. Up to 300 feet within the data center. Note that, because of wiring channel locations and other factors, the wiring distance between data center racks may be substantially longer than a simple straight line.

Billing. Monthly, per cross connect.

Required
- *Copper Cross Connect - San Francisco - Installation (DC-NWU2-XCC-1T)*

2.4.2.5   Hotel Rack (1U) - Managed Colo - San Francisco (DC-RKU2-RK-HR)

This service provides Customer with one (1) rack unit (RU) in a shared rack within a Virtustream data center. Included with this service are 2x 1G Copper interfaces.

Billing. Monthly, per 1U slot.

Required, one of the following:

- *Remote Eyes & Hands (US) - Bronze (DC-SVC-REU-B)*
- *Remote Eyes & Hands (US) - Silver (DC-SVC-REU-S)*
- *Remote Eyes & Hands (US) - Gold (DC-SVC-REU-G)*

2.4.3   Remote Management

2.4.3.1   Remote Eyes & Hands (US) - Bronze (DC-SVC-REU-B)

This service provides Customer with access to two hours per month of on-site data center technician service at one of Virtustream's US data centers. This service can be used to enable Virtustream to perform manual tasks that require direct, hands-on contact with equipment in colo or hotel space. Bronze-level on-site service at Virtustream's U.S. data centers is provided during business hours (9:00am to 5:00pm, M-F).

Billing is monthly for the base rate (per customer's contract), plus additional service hours used beyond two hours, in 15-minute increments (rounded up).

Related

- *Hotel Rack (1U) - Managed Colo - Vienna (DC-RKU1-RK-HR)*
- *Hotel Rack (1U) - Managed Colo - San Francisco (DC-RKU2-RK-HR)*

- *Hotel Rack (1U) - Managed Colo - Las Vegas (DC-RKU3-RK-HR)*

2.4.3.2   Remote Eyes & Hands (US) - Silver (DC-SVC-REU-S)

This service provides Customer with access to five hours per month of on-site data center technician service at one of Virtustream's US data centers. This service can be used to enable Virtustream to perform manual tasks that require direct, hands-on contact with equipment in colo or hotel space. Silver-level on-site service at Virtustream's U.S. data centers is provided during business hours (9:00am to 5:00pm, M-F).

Billing is monthly for the base rate (per customer's contract), plus additional service hours used beyond five hours, in 15-minute increments (rounded up).

Related

- *Hotel Rack (1U) - Managed Colo - Vienna (DC-RKU1-RK-HR)*
- *Hotel Rack (1U) - Managed Colo - San Francisco (DC-RKU2-RK-HR)*
- *Hotel Rack (1U) - Managed Colo - Las Vegas (DC-RKU3-RK-HR)*

2.4.3.3   Remote Eyes & Hands (US) - Gold (DC-SVC-REU-G)

This service provides Customer with access to 10 hours per month of on-site data center technician service at one of Virtustream's US data centers. This service can be used to enable Virtustream to perform manual tasks that require direct, hands-on contact with equipment in colo or hotel space. Gold-level on-site service at Virtustream's U.S. data centers is provided 24 hours a day, 7 days a week.

Billing is monthly for the base rate (per customer's contract), plus additional service hours used beyond ten hours, in 15-minute increments (rounded up).

Related

- *Hotel Rack (1U) - Managed Colo - Vienna (DC-RKU1-RK-HR)*
- *Hotel Rack (1U) - Managed Colo - San Francisco (DC-RKU2-RK-HR)*
- *Hotel Rack (1U) - Managed Colo - Las Vegas (DC-RKU3-RK-HR)*

2.4.3.4   Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (15 Minutes) (DC-SVC-REU-SAHQ)

15-minute increments of US Bronze or Silver service.

Billing per service increments rendered.

2.4.3.5   Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (1 Hour) (DC-SVC-REU-SAH1)

One-hour increments of US Bronze or Silver service.

Billing per service increments rendered.

2.4.3.6   Remote Eyes & Hands (US) - Gold Ad Hoc (15 Minutes) (DC-SVC-REU-GAHQ)

15-minute increments of US Gold service.

Billing per service increments rendered.

2.4.3.7   Remote Eyes & Hands (US) - Gold Ad Hoc (1 Hour) (DC-SVC-REU-GAH1)

One-hour increments of US Gold service.

Billing per service increments rendered.

3   PLATFORM OPERATIONS RESPONSIBILITIES

The parties' responsibilities after Onboarding are summarized in the table below.

Table 3-1. Platform Operations Responsibilities		
Task	Customer	Virtustream
Submit firewall change requests with valid information and Customer internal approval	R	C
Implement firewall change requests	C	R
Submit load balancing change requests with valid information and Customer internal approval	R	C
Implement load balancing change requests	C	R
Maintain network routing domain within Customer premise	R	C
Assign Internet Protocol subnets within Virtustream Data Centers	C	R
Manage Internet Protocol address assignments within Customer dedicated subnets	R	C
Maintain OS and Application security to avoid resource misuse due to security incidents	R	C
Submit VPN change requests with valid information and Customer internal approval	R	C
Implement VPN change requests	C	R
Define backup schedules, retentions, and policies	R	S
Configure backups based on requirements	C	R
Troubleshoot application issues for Customer installed and managed applications	R	C
Install and manage guest OS and application	R	C
Submit backup restore requests with valid information	R	C
Perform backup restores	C	R
Verify backup restore results	R	C
Secure the proper access rights or maintenance and support services with respect to any component (e.g., hardware, software, network, maintenance) installed or managed by Customer	R	I

R: Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
A: Accountable is the authority who approves the work of R before it is effective.
S: Support R as necessary to complete the task or deliverable.
C: Consulted reviews output or progress necessary to complete the task or deliverable.
I: Informed needs to be notified of results, completion, or deliverable but need not necessarily be consulted.
NOTE: When Virtustream is In the Support role or Consulted, Virtustream may charge Customer T&M for resources used.

4   CHANGE CONTROL PROCEDURES; THIRD PARTY MATERIALS

4.1   Notice of Changes

Virtustream will give Customer advance notice of any changes being applied to Services that may affect Customer in accordance with Virtustream's change management procedures. Notices of changes are disseminated by Virtustream through means of electronic mail distribution lists and other appropriate media as determined by Virtustream. If Emergency Maintenance is required due to an Incident, Virtustream will give Customer notice as is reasonably possible, without impeding the resolution of the Incident.

5 SERVICE LEVEL FRAMEWORK

The service levels ("Service Levels") applicable to the Services specified in Sections 1 and 2 are set forth in Schedule B to this SD ("Service Levels for Cloud Platform Services"). The framework that governs all Service Levels is set forth in this Section.

5.1 Commencement of Service Levels

Commencing thirty (30) days from the Service Start Date (as set forth in the applicable Order Form), Virtustream's performance of the Services will meet each applicable Service Level. If Virtustream's performance of the Services does not meet the applicable Service Level, then Virtustream will use commercially reasonable efforts to restore its performance to meet such Service Level.

5.2 Service Level Reports

Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.

5.3 Service Level Review Meetings

Monthly Service Level review meetings will be conducted by Virtustream with Customer where the monthly Service Level report specified above will be discussed. If any of the Service Levels measured over the previous calendar month period is not achieved in that month, then Virtustream will include the steps taken to rectify the problem in the next monthly Service Level Report. In addition, the issue shall be an agenda topic for discussion at the next monthly service review meeting. Additionally, after restoring service or otherwise resolving any immediate problem as specified in this SD, if Virtustream fails to provide Services in accordance with the Service Levels, Virtustream shall:

a. Promptly investigate and report on the causes of such problem;

b. Provide a Root Cause Analysis of such failure as soon as practical after such failure or at Customer's request;

c. Correct such problem that is Virtustream's fault or responsibility, as soon as reasonably practicable and coordinate the correction of such problem if Virtustream does not have responsibility for the cause of such problem.

d. Advise Customer of the status of remedial efforts being undertaken with respect to such problem;

e. Demonstrate to Customer's reasonable satisfaction that the causes of such problem (that is Virtustream's fault or responsibility) have been or shall be corrected on a permanent basis; and

f. Take corrective actions to prevent any recurrence of such problem (that is Virtustream's fault or responsibility).

5.4   Root Cause Analysis

Promptly following Virtustream's failure to meet a Service Level, Virtustream will perform a root cause analysis to determine the reason for that failure. Upon Virtustream's determination of the cause of such failure, it will provide to Customer a preliminary report citing the cause of such failure. If Virtustream determines that the failure was due to Virtustream, an additional report will be provided that details the root causes of the failure, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. Virtustream will correct the problem and use reasonable commercial efforts to minimize the re-occurrence of such failures.

5.5   Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

a. A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

b. Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);

c. Any hardware, software or other product of a third-party or Customer equipment;

d. Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;

e. Downtimes resulting from a Virtustream's scheduled maintenance windows;

f. Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;

g. Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date;

h. An election by Customer to purchase a base commitment that is not sufficient to run Customer's system (e.g., If a customer elects to size a μVM pool that is insufficient to run the designated workload);

i. Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply;

j. Cloud Cover Services (CCS) offerings — for which the Service Level Objectives (SLOs) do not apply;

k. Resolution delays due to lack of client response and/or Customer provided credential based information;

l. Priority levels not agreed upon by both customer and supplier;

m. Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

6 CPS SERVICE DESK

Virtustream Service Desk Contact Details	
Hours of Support	24 x 7 x 365
Contact Number	1-877-303-9524
Email Address	XOC@virtustream.com
Service Management Dashboard	https://dashboard.virtustream.com
Language	English

6.1 Overview

The Virtustream Service Desk will perform the primary functions of responding to service requests and Incidents. Primary contact shall be via email. Toll-free telephone support and a Service Management Dashboard, which provides access to a ticketing self-service portal shall also be made available. Only representatives nominated during the onboarding process or through a service request will be able to report Incidents or Request Services via the Service Desk.

All tickets logged via email are considered a Service Request unless Customer informs the service desk that the problem is an Incident.

6.1.1 Incidents

Virtustream's Service Desk will respond to incidents reported by Virtustream's Monitoring software or by Customer ("Incidents") in the manner set forth in 5.4 ("Incident Reporting Process," p. 71), notify Customer if Virtustream becomes aware of the Incident prior to notification from Customer, and develop a resolution plan (see 5.1 "Resolution Plan").

See the Incident Management RACI table on page 73 for more information about the roles of Customer and Virtustream.

6.1.2 Service Requests

Virtustream's Service Desk will respond to service requests from Customer and resolve the request in the manner set forth in 5.5 ("Service Request Process" p. 71). All service requests must be submitted via a service desk request.

6.2 Support Schedule

Nominated representatives can always contact the service desk. Monitoring and notification is always 24 x 7 x 356. Responses to Incidents and service requests will be carried out during the times listed in the table below.

NOTE: Customers who subscribe to Virtustream's Cloud Cover Services (CCS) should refer to the CCS SD for details on applicable OS, Database, and SAP Basis support.

Table 5-1. Support Schedule	
Monitoring	24 x 7 x 365
Notification	
Responses to Service Requests	Monday-Friday, 8 AM EST - 6 PM (in Customer time zone)
Responses to Incidents	24 x 7 x 365
Notes	Full support, and overnight monitoring and emergency support as needed. Overnight support requires a ticket, along with escalation from an authorized representative by phone to the Service Desk. Any emails or XOC tickets sent after normal business hours without a call to the Service Desk for escalation by an authorized user will be handled on the next business day.

6.3 Service Management Dashboard

Virtustream shall provide a service management dashboard ("Service Management Dashboard"), accessible with Virtustream-provided credentials. The Service Management Dashboard shall provide access to applets that allow Customer to create and update service management requests and to report Incidents. The dashboard shall also provide access to a standardized display for some of the foundational infrastructure monitoring, if those Services have been purchased by Customer. Customer dashboards are available via professional services engagement. Dashboard user credentials can be requested via the Virtustream service desk by Customer's nominated representatives to the Virtustream service desk.

6.4 Incident Reporting Process

To report an Incident, one of Customer's nominated representatives will contact the Virtustream service desk via telephone, email, or via the Service Management Portal using the contact details set forth above ("Virtustream Service Desk Contact Details"). Where initial contact is via telephone, Customer will provide additional details via email to the email address above. In the event Virtustream becomes aware of the Incident prior to notification from Customer, Virtustream shall provide email notification to Customer of the occurrence of the Incident. Following the response, Virtustream will conduct an initial analysis, and prepare a resolution plan and outline the steps needed to resolve the issue, and an estimated fault resolution time.

6.4.1 Resolution Plan

Virtustream will develop a resolution plan which will be communicated to Customer via the Virtustream service desk.

6.5 Service Request Process

Service requests shall be submitted by one of Customer's nominated representatives to the Virtustream service desk.

Virtustream shall provide a response to such service request received from, or approved by, nominated representatives with the within sixty (60) minutes. Virtustream shall within one (1) business day of such request inform Customer of the anticipated completion date and time of such service request. Time frames will vary based on nature of the service request. Unless otherwise agreed by the parties, service requests are not reviewed outside of normal business hours (Monday-Friday, 8AM-5PM ET), without prior written agreement of Virtustream.

6.6 Incident & Service Request Prioritization

6.6.1 Escalations within Virtustream

Virtustream will provide Level I support and first call resolution where possible, as determined by Virtustream. (Level 1 support is defined as the Virtustream xOC help desk, which is staffed 24x7x365 to respond to customer phone calls, emails and tickets. First call resolution is Virtustream's commitment to taking the necessary actions to restore service upon first contact with the Service Desk.) Where first call resolution is not possible, the Virtustream service desk provides incident management for Incidents and urgent service requests escalated to Level II and Level III resources as defined below.

In the event that Virtustream's response to an Incident is not acceptable to Customer, Customer can contact the Virtustream service desk and request escalation. Virtustream shall, upon receipt of any such request, immediately escalate the issue to the head of the service desk or technical team as appropriate.

6.6.2 Service Request Prioritization

Service requests are assigned a priority of either 'Urgent' or 'Standard' and are queued for fulfillment with the corresponding priority. All service requests will be reviewed by the Virtustream service desk, who will determine the appropriate priority to assign with Customer collaboration.

6.6.3 Incident Prioritization

All Incidents that are reported to the Virtustream service desk, or that Virtustream otherwise becomes aware of, will be initially assigned a priority by the Virtustream service desk as set forth in the two tables below. Internal escalation for Incidents to Level II and Level III resources are based on the priority level assigned to the Incident.

Table 5-2. Definition of Priority Levels	
Priority	**Definition**
1	SLO is a Service level objective, which is a target timeframe.
2	SLA is a Service level agreement, which is a contractual, agreed-upon timeframe.
3	Time to assign indicates the timeframe to send automated system acknowledgement that the ticket has been logged and assigned.
4	Target response time indicates the timeframe for an engineer to review the issue and respond with a technical plan.

Table 5-3. Incident Priority Definition Matrix						
	IMPACT					
URGENCY	*Many Customers / Many Services*	*Many Services / One Customer*	*One Customer / One Service*	*Significantly Reduced Availability*	*Reduced Availability*	*Reduced Performance*
Extremely time-sensitive (C)	P1	P1	P1	P2	P2	P2
Very time-sensitive (H)	P1	P1	P2	P2	P2	P3
Immediate Need (M)	P1	P2	P2	P2	P3	P3
Time-sensitive (L)	P2	P2	P3	P3	P3	P4
None	P3	P3	P4	P4	P4	P4

6.7 Service Desk Response Times

Subject to any Service Level Exception, Virtustream will respond to an Incident within the response time set forth below 95% of the time.

See 5.6.3 ("Incident Prioritization," p. 72) for priority level definitions.

Table 5-4. Enterprise-level Agreements			
	Virtustream SLA	**Virtustream SLO**	**Virtustream SLO**
Ticket Priority	**Time to Assign (ticket acknowledgement)**	**Target Response time (technical response)**	**Target Resolution (issue resolution)**
Priority 1	5 minutes	30 minutes	4 hours
Priority 2	5 minutes	60 minutes	8 hours
Priority 3	5 minutes	4 hours	1 business day
Priority 4	5 minutes	8 business hours	3 business days

6.7.1 Technical Response Definitions

Table 5-5. Technical Response Definitions and Timing		
Priority/ Severity	**Definition**	**Response Time**
1	Major part of the system is unavailable/not operating correctly, affecting multiple users. No workarounds in place and business operations are not possible. **OR** Incident has a critical impact on the business (e.g., loss of the Exchange Production server impacting all users).	**30 minutes**
2	Part of the system is unavailable/not operating correctly, affecting users in a single function. No workarounds in place and business operations in this function are not possible/severely impacted. **OR** Incident has a serious impact on part of the business (e.g., a configuration change is impacting a small subset of users).	**60 minutes**
3	Part of the system is unavailable/not operating correctly, affecting users in a single function. Workarounds in place, but business operations are impacted, although not severely. **OR** Incident has a temporary impact on users and is non critical or is a development issue (e.g., email is slow to deliver)	**4 hours**
4	Incident that is causing inconvenience to the business, but not impacting operations. **OR** Incident has a minor impact on users or business, or issue is a request for further information	**8 business hours**

6.8   Problem Management

In the event that a Customer is experiencing a problem, Customer may request a Root Cause Analysis ("RCA") ticket by contacting the Virtustream technical account manager ("TAM"). Virtustream will produce a preliminary RCA for all in-scope P1 Incidents within 48 hours, and a final report within 15 calendar days. Virtustream will investigate and diagnose the problem with the support of Customer and the RCA.

Table 5-6. Incident Management RASCI		
Role/Function	Customer	Virtustream
Incident Management		
Document, track and manage all Incidents using ITSM system (ITIL methodology/practices)	S	R/A
Perform Incident management related services necessary to meet Service Levels	S	R/A
Assign Incident priority based on impact and standards set forth above	S	R/A
Provide method of collaboration to address high priority Incidents (e.g. P1 bridge)	S	R/A
Communicate to Customer on the progress made to resolve Incidents and applicable workarounds	S	R/A
Provide recommendations to avoid the reoccurrence of Incidents, develop and update knowledge base articles	S	R/A

R: Responsible for ensuring that the task or deliverable is completed accurately and timely; the "doer."
A: Accountable is the authority who approves the work of R before it is effective.
S: Support R as necessary to complete the task or deliverable.
C: Consulted reviews output or progress necessary to complete the task or deliverable.
I: Informed needs to be notified of results, completion, or deliverable but need not necessarily be consulted.
NOTE: When Virtustream is In the Support role or Consulted, Virtustream may charge Customer T&M for resources used.

7 DEFINITIONS

Disaster Recovery Protection: Core μVMs and Storage Replication are protected in the case of a Disaster Recover (DR) Event. Compute resources in Customer's secondary Virtustream data center are reserved to replicate core μVMs from Customer's primary Virtustream data center.

DR (Disaster Recovery) Event: In the case of a catastrophic failure at a Virtustream data center, Virtustream may declare a DR event.

Dual Site: means live/operational resources are presentable within two data centers — a single instance of which may run live/operational at the primary data center or, in a recovery mode or disaster mode, at the secondary data center.

Emergency Maintenance: Periods of time, during the term of an applicable Order Form, that full access to and use of the Services is interrupted or otherwise unavailable due to maintenance activities that Virtustream must perform, within the timeframe that is not fit into the Scheduled Outages notification window, to restore services or address known critical risks. For the avoidance of doubt, all Emergency Maintenance (including the dates and maximum duration thereof) must be communicated by Virtustream to Customer with written notice prior to the maintenance events. Virtustream must use its best efforts to minimize the duration of any interruption or unavailability of the Services.

HA: High Availability.

High Availability within Data Center: in the event of a host failure, Virtustream will restart VMs that were running on the failed host on another host within the Virtustream cloud.

Mbps: the measure of network bandwidth measured in Mega-bits per second.

μVM (pronounced "micro VM"): a Virtustream computing processing unit consisting of CPU, memory, storage (in IOPS), and associated LAN network bandwidth (in Mbps).

μVM Resource Pool: The aggregated physical compute hardware — CPU and memory, as well as other components — allocated to a set of μVMs in a Virtustream virtual infrastructure.

IOPS: input/output operations per second for storage devices.

LAN: Local Area Network implemented within a Virtustream Data Center; does not include connectivity between Virtustream Data Centers or between a Virtustream Data Center and a Customer's location.

Level 0 support: self-service tools available to the Customer to report a service disruption

Level 1 support: the Virtustream xOC help desk, which is staffed 24x7x365 to respond to Customer phone calls, emails, and tickets.

Non-Replicated: Customer data is not replicated to an alternative IaaS Platform**.**

Restoration or Restore: The time to fully restore failed Services, as measured from the point at which a DR Event has been declared by Customer.

Scheduled Outages: Periods of time, during the term of an applicable Order Form, that full access to and use of the Services is interrupted or otherwise unavailable due to (a) scheduled upgrades or maintenance to the Virtustream network or Virtustream's equipment, or (b) any other mutually agreed upon reason or purpose; provided, that, in order for an interruption or other unavailability of access to and use of the Services to remain qualified as a Scheduled Outage, Virtustream must use its best efforts to minimize the duration of any interruption or unavailability of the Services. For the avoidance of doubt, all Scheduled Outages (including the dates and maximum duration thereof) due to scheduled upgrades or maintenance must be communicated by Virtustream to Customer with written notice of at least seven (7) calendar days. Emergency Maintenance is not a Scheduled Outage.

Single Site: live/operational resources are available within a single Virtustream Data Center.

Site: premises or location to and from where Virtustream agrees to provide the Service.

Storage: an amount of disk storage, which is agreed by Virtustream to be provisioned to Customer based on which to locate Customer data and VMs.

Storage Replication: means where data is replicated in near real time from the primary *x*Stream environment to a secondary *x*Stream environment,

Virtustream Data Center: The Virtustream facility or facilities from which Services are provided.

Virtual Machine or VM: a virtual machine, sometimes referred to as a virtual server, existing within the Virtustream's Cloud Platform.

VPN: Virtual Private Network.

Virtustream IaaS Service Platform: Virtustream's cloud computing platform which provides Customer with a secure cloud computing capability in a multi-tenanted environment.

For RASCI charts:

Responsible: the party responsible for ensuring that the task, function, or deliverable described is completed accurately and timely; often known as the "doer."

Accountable: the party to whom "R" is accountable and is the authority who approves or signs off on work before it is effective.

Support: the party who provides resources or plays a supporting role to the extent reasonably necessary to complete the task, function, or deliverable. When Virtustream is in the Support role, Virtustream may charge Customer on a time and materials basis for its resources used to "Support."

Consulted: the party who reviews output or progress necessary to complete the task, function, or deliverable. When Virtustream is "Consulted," Virtustream may charge Customer on a time and materials basis for its resources used to "Consult."

Informed: the party who needs to be notified of results, completion, or deliverable, but need not necessarily be consulted.

8   SCHEDULE A - SCOPE OF CLOUD PLATFORM SERVICES

8.1   µVM Features

This chart describes overall features offered with the µVMs. The Order Form shall set forth Customer's specific selected µVMs.

Table 7-1. µVM Features		
Feature / Characteristic	Enterprise Basic Plus µVM	Enterprise Reserve µVM
Has an Availability Service Level	YES	YES
Storage Replication can be provided at an additional cost	YES	N/A
High Availability within Data Center	YES	YES
Disaster Recovery Protection	NO	YES (provided Customer also purchases Tier 0, I, II, or III Block Storage - Replicated)
Site Resources	Primary Site	Secondary Site

8.1.1   Base Commitment and On Demand

The Service volumes (which consists of Basic Plus µVMs) as of the Service Start Date are set forth in the applicable Order Form ("Base Commitment"). In the event Customer needs µVMs that exceed the Base Commitment, they will automatically be consumed and Customer will be billed at the same rate for those µVMs as for the Base Commitment. An overage of up to 20% of the Base Commitment will have the same Availability as the Base Commitment. Virtustream does not guarantee Availability of additional µVMs beyond this +20% overage buffer, and such additional µVMs will not be used in computing Service Availability (see 8.1).

8.2   Storage Features

Table 7-2. Storage Features				
Feature / Characteristic	Tier 0	Tier 1	Tier 2	Tier 3
Storage Latency Service Level	≤ 3ms	≤ 10ms	≤ 20ms	≤ 40ms (SLO)
Storage Replication Available at extra cost when choosing the "replicated" option	YES	YES	YES	YES
High Availability Within Data Center	YES	YES	YES	YES

8.2.1   Base Commitment and On Demand

8.2.1.1   Storage Volume

The storage volumes (which consists of Tier 0/1/2/3 storage in per GB quantities) as of the Service Start Date are set forth in the applicable Order Form ("Storage Base Commitment").

8.2.1.2   Overage

In the event Customer needs storage that exceeds the Storage Base Commitment, they will automatically be consumed and Customer will be billed at the same rate for that storage on a per GB basis as for the Storage Base Commitment. Virtustream does not guarantee Availability of Storage Base Commitment of such additional storage and such additional storage will not be used in computing Storage Latency Service Level.

8.2.1.3   Disk Geometries

Notwithstanding the table above, Virtustream reserves the right at any time, without notice, to change the underlying disk technologies and geometries. In the event Virtustream changes underlying disk technologies and geometries, Virtustream's Service Levels for Storage I/O and Latency will not be changed.

9 SCHEDULE B - SERVICE LEVELS FOR CLOUD PLATFORM SERVICES

The following Service Levels are applicable to the Cloud Platform Services provided under this Service Description.

9.1 µVM Service Availability

Service Availability expressed as a percentage is calculated per the formula below. The calculation is performed separately, for Core µVMs and Basic µVMs. "Availability" or "Available" are subject to the terms of the calculation below, and subject to any Service Level Exception — meaning that the applicable µVM, storage, and network access within Virtustream's data center is available to Customer.

$$\frac{(\text{T x Customer } \mu\text{VMs}) - (\text{U x Unavailable Customer } \mu\text{VMs})}{\text{T x Customer } \mu\text{VMs}} \times 100$$

Where,

T = The total number of minutes within the applicable month, less the minutes (or portion thereof) for any Scheduled Outages.

Customer µVMs = the number of applicable µVMs, storage, and network access to which Customer entitled in the applicable calendar month.

U = the number of minutes (or portion thereof) that any applicable µVMs, storage, and network access are not available to Customer in the applicable calendar month. This excludes any unavailability due to Scheduled Outages.

Unavailable Customer µVMs = the number of applicable µVMs, storage, and network access that are unavailable to Customer in the applicable calendar month. If there is a network or storage failure that prevents access to any µVMs those µVMs will be considered unavailable until the failure has been resolved.

Table 8-1. µVM Availability		
	Enterprise Basic Plus µVM	Enterprise Reserve µVM
Availability	99.99%	N/A

Subject to any Service Level Exceptions set forth in this Service Description, the table below sets forth additional Service Levels for Services described herein.

Table 8-2. Service Levels		
Category	Service Description	Service Level
LAN / WAN Service Level Availability	WAN Circuit from Virtustream Data Center to Customer site	Service levels of the applicable third party carrier is passed through to Customer
	Local Area Network [internal to Virtustream Data Center]	99.999%
Restoration of service due to a host failure within the Virtustream cloud	Time to Restore failed VMs (VM is re-executed on another host server and back to 'ready' state.	100% within 5 minutes
Data Storage & Data Backup	For Storage Replication, data replicated to one of the alternate Data Centers	100% of data is replicated from primary to secondary Virtustream Data Centers within 15 minutes

Category	Service Description	Service Level
	Data backed up in accordance with Customer's policy	100% of data backed up
	Backed up data replicated to one of the alternate Virtustream Data Centers in accordance with Customer's policy	100% of backups are copied from primary to secondary Virtustream Data Centers
	Time taken to initiate Restoration from back up	Restore initiated within 4 hours of Customer request
	Average Storage Latency	Tier 0: 3ms Tier I: 10ms Tier II: 20ms Tier III: 40ms (service objective)
VMs (Virtual Servers)	Windows, Red Hat, or SUSE Virtual Servers (running operating system instances)	(a) 99.9% for VMs running with Enterprise Basic Plus µVMs
Firewalls	Virtual firewalls, dedicated virtual context (FWSM), virtual firewall contexts, or physical firewall configured in HA pairs	Available 99.999% with throughput consistent with service order, less than 30ms latency, and less than 3% packet loss
Load Balancers	Virtual or physical load balancers configured in HA pairs	Available 99.999% with throughput consistent with service order, less than 30ms latency, and less than 3% packet loss
Monitoring, Response, & Notification	Availability Monitoring. Virtustream will monitor for service availability of all devices/services for which an uptime and/or performance SLA is defined. Fault Monitoring. Virtustream monitors status events on servers and network devices including availability, process status, file system capacity, and backup success/failure. Virtustream will also monitor for server hardware faults. Performance Monitoring. Virtustream monitors key performance metrics for the operating system (e.g., CPU, RAM, and Disk), and select applications (e.g., process statistics, users, throughput) and databases (e.g., caching, performance, transaction success). Security Monitoring. Virtustream will actively monitor the Virtustream infrastructure and services for vulnerabilities and proactively remediate any identified vulnerabilities. Virtustream will provide security-focused monitoring of customer devices and environments in alignment to the security services Customer purchases from Virtustream	Virtustream will notify Customer of any alerts that affect service and device availability or performance within 30 minutes of the alert.

9.2   Physical HANA Appliance Service Availability

Service Uptime expressed as a percentage is calculated as follows for HANA Appliance Availability. "Availability," subject to the terms of the calculation below, and subject to any Service Level Exception, means that the applicable μVMs, storage, and network access within Virtustream's data center is available to Customer.

$$\frac{(T \text{ x Customer HANA Appliances}) - (U \text{ x Unavailable Customer HANA Appliances})}{T \text{ x Customer HANA Appliances}} \text{ X } 100$$

Where,

T is the total number of minutes within the applicable month, less the minutes (or portion thereof) for any Scheduled Outages.

Customer HANA Appliances is the number of HANA Managed Appliances to which Customer is entitled in the applicable calendar month.

U is the number of minutes (or portion thereof) that any applicable HANA Appliances are not available to Customer in the applicable calendar month. This excludes any unavailability due to Scheduled Outages.

Unavailable Customer HANA Appliances is the number of applicable HANA Appliances that are unavailable to Customer in the applicable calendar month. If there is a network or storage failure that prevents access to any HANA Appliances, those HANA Appliances will be considered unavailable until the failure has been resolved.

Table 8-3. Physical HANA Availability		
SLA Area	**Description**	**Performance Metric**
Physical HANA Appliance Uptime: with HA	Physical HANA hardware with high availability configuration (N+1)	99.95%
Physical HANA Appliance Uptime: No HA	Physical HANA hardware without high availability configuration (N+0)	99.5%

9.3   Storage Latency

Storage latency is expressed, in milliseconds, as the average latency calculated in accordance with the formula below across a 5 minute interval, separately for Tier 0, Tier I, Tier 2, and Tier 3 storage.

$$\text{Average Latency } = \frac{Reads \text{ x } RL + Writes \text{ x } WL}{IOPS}$$

Where

Reads = Read (input) operations

Writes = Write (output) operations

- RL = Average read latency (time) per operation
- WL = Average write latency (time) per operation
- IOPS = Total number (reads + writes) of I/O operations

9.4   Service Level Credits

      i)   Subject to any Service Level Exception set forth in Section 9.5, and this Section, Virtustream will provide to Customer a Service Level Credit for any month in which Virtustream fails to meet the applicable Service Level (each such failure, a "Service Level Failure") as set forth below.

µVM Availability on Enterprise Basic Plus µVM	Service Level Credit*
>99.95% and <99.99%	1%
>99.9% - 99.95%	3%
95% - 99.9%	5%
90% - 94.99%	10%
below 90%, or if, the µVMs specified in applicable Order Form are not Available for a consecutive 8 hour period.	15%

*percentage of monthly fees of the µVMs under the applicable monthly invoice

Tier 1 Storage Latency (ms)	Tier 2 Storage Latency (ms)	Service Level Credit*
>10 and ≤15	>20 and ≤25	2%
>15 and ≤20	>25 and ≤30	5%
>20 and ≤30	>30 and ≤40	10%
>30	>40	15%

* percentage of monthly fees of the affected storage under the applicable monthly invoice

      (ii)   Where a single Incident results in more than one Service Level Failure, Virtustream will provide Customer with only the largest Service Level Credit. Customer will not be entitled to Service Level Credits for each of such Service Level Failures.

      (iii)   Virtustream will credit any Service Level Credit against the charges otherwise payable by Customer to Virtustream, on the next invoice with respect thereto. If no further charges are due and owing to Virtustream, Virtustream shall pay Customer the applicable Service Level Credit within forty-five (45) calendar days of the date such credit was incurred.

      (iv)   If Customer's accounts receivable balance is not current in the month in which the Service Level Failure occurred (i.e. Customer has not paid its invoices in accordance with the terms of the MSA), Customer shall not be entitled to a Service Level Credit, and Virtustream will be excused for its failure to meet or exceed the Service Levels.

      (v)   In no event will the aggregate of all Service Level Credits paid under an Order Form in any month exceed fifteen percent (15%) of the total fees payable for such month pursuant to the applicable monthly invoice.

9.5   Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

    a.   A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

b.   Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);

c.   Any hardware, software or other product of a third-party or Customer equipment;

d.   Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;

e.   Downtimes resulting from a Virtustream's scheduled maintenance windows;

f.   Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;

g.   Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date;

h.   An election by Customer to purchase a base commitment that is not sufficient to run Customer's system;

i.   Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply;

j.   Cloud Platform Services (CPS) offerings — for which the Service Level Objectives (SLOs) do not apply;

k.   Resolution delays due to lack of client response and/or Customer provided credential based information;

l.   Priority levels not agreed upon by both customer and supplier;

m.   Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

10 SCHEDULE C - END USER LICENSE TERMS

10.1 Microsoft

Microsoft | Volume Licensing

END USER LICENSE TERMS

TERMS AND CONDITIONS REGARDING USE OF MICROSOFT SOFTWARE

This document governs the use of Microsoft software, which may include associated media, printed materials, and "online" or electronic documentation (individually and collectively, "Products") provided by Virtustream, Inc. (hereinafter referred to as "Customer"). Customer does not own the Products and the use thereof is subject to certain rights and limitations of which Customer must inform you. Your right to use the Products is subject to the terms of your agreement with Customer, and to your understanding of, compliance with, and consent to the following terms and conditions, which Customer does not have authority to vary, alter, or amend.

1. **DEFINITIONS.**

   "Client Software" means software that allows a Device to access or utilize the services or functionality provided by the Server Software.

   "Device" means each of a computer, workstation, terminal, handheld PC, pager, telephone, personal digital assistant, "smart phone," server or other electronic device.

   "Server Software" means software that provides services or functionality on a computer acting as a server.

   "Software Documentation" means any end user document included with server software.

   "Redistribution Software" means the software described in Paragraph 4 ("Use of Redistribution Software") below.

2. **OWNERSHIP OF PRODUCTS.** The Products are licensed to Customer from an affiliate of the Microsoft Corporation (collectively "Microsoft"). All title and intellectual property rights in and to the Products (and the constituent elements thereof, including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Products) are owned by Microsoft or its suppliers. The Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Your possession, access, or use of the Products does not transfer any ownership of the Products or any intellectual property rights to you.

3. **USE OF CLIENT SOFTWARE.** You may use the Client Software installed on your Devices by Customer only in accordance with the instructions, and only in connection with the services, provided to you by Customer. The terms of this document permanently and irrevocably supersede the terms of any Microsoft End User License Agreement that may be presented in electronic form during your use of the Client Software.

4. **USE OF REDISTRIBUTION SOFTWARE.** In connection with the services provided to you by Customer, you may have access to certain "sample," "redistributable" and/or software development ("SDK") software code and tools (individually and collectively "Redistribution Software"). **YOU MAY NOT USE, MODIFY, COPY, AND/OR DISTRIBUTE ANY REDISTRIBUTION SOFTWARE UNLESS YOU EXPRESSLY AGREE TO AND COMPLY WITH CERTAIN ADDITIONAL TERMS CONTAINED IN THE SERVICES PROVIDER USE RIGHTS ("SPUR") APPLICABLE TO CUSTOMER, WHICH TERMS MUST BE PROVIDED TO YOU BY CUSTOMER.** Microsoft does not permit you to use any Redistribution Software unless you expressly agree to and comply with such additional terms, as provided to you by Customer.

5. **COPIES.** You may not make any copies of the Products; provided, however, that you may (a) make one copy of Client Software on your Device as expressly authorized by Customer; and (b) you may make copies of certain Redistribution Software in accordance with Paragraph 4 (Use of Redistribution Software). You must erase or destroy all such Client Software and/or Redistribution Software upon termination or cancellation of your agreement with Customer, upon notice from Customer or upon transfer of your Device to another person or entity, whichever occurs first. You may not copy any printed materials accompanying the Products.

6. **LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION AND DISASSEMBLY.** You may not reverse engineer, decompile, or disassemble the Products, except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.

7. **NO RENTAL.** You may not rent, lease, lend, pledge, or directly or indirectly transfer or distribute the Products to any third party, and may not permit any third party to have access to and/or use the functionality of the Products except for the sole purpose of accessing the functionality of the Products in the form of software services in accordance with the terms of this agreement and any agreement between you and Customer.

8. **TERMINATION.** Without prejudice to any other rights, Customer may terminate your rights to use the Products if you fail to comply with these terms and conditions. In the event of termination or cancellation of your agreement with Customer or Customer's agreement with Microsoft under which the Products are licensed, you must stop using and/or accessing the Products, and destroy all copies of the Products and all of their component parts.

9. **NO WARRANTIES, LIABILITIES OR REMEDIES BY MICROSOFT. ANY WARRANTIES, LIABILITY FOR DAMAGES AND REMEDIES, IF ANY, ARE PROVIDED SOLELY BY CUSTOMER AND NOT BY MICROSOFT, ITS AFFILIATES OR SUBSIDIARIES.**

10. **PRODUCT SUPPORT.** Any support for the Products is provided to you by Customer and is not provided by Microsoft, its affiliates or subsidiaries.

11. **NOT FAULT TOLERANT.** THE PRODUCTS MAY CONTAIN TECHNOLOGY THAT IS NOT FAULT TOLERANT AND ARE NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE IN ENVIRONMENTS OR APPLICATIONS IN WHICH THE FAILURE OF THE PRODUCTS COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL, PROPERTY OR ENVIRONMENTAL DAMAGE.

12. **EXPORT RESTRICTIONS.** The Products are subject to U.S. export jurisdiction. Customer must comply with all applicable laws including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. For additional information, see http://www.microsoft.com/exporting/.

13. **LIABILITY FOR BREACH.** In addition to any liability you may have to Customer, you agree that you will also be legally responsible directly to Microsoft for any breach of these terms and conditions.

10.2   Red Hat

END USER LICENSE AGREEMENT
RED HAT® ENTERPRISE LINUX® AND RED HAT APPLICATIONS

![redhat logo]

PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY BEFORE USING SOFTWARE FROM RED HAT. BY USING RED HAT SOFTWARE, YOU SIGNIFY YOUR ASSENT TO AND ACCEPTANCE OF THIS END USER LICENSE AGREEMENT AND ACKNOWLEDGE YOU HAVE READ AND UNDERSTAND THE TERMS. AN INDIVIDUAL ACTING ON BEHALF OF AN ENTITY REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO ENTER INTO THIS END USER LICENSE AGREEMENT ON BEHALF OF THAT ENTITY. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN YOU MUST NOT USE THE RED HAT SOFTWARE. THIS END USER LICENSE AGREEMENT DOES NOT PROVIDE ANY RIGHTS TO RED HAT SERVICES SUCH AS SOFTWARE MAINTENANCE, UPGRADES OR SUPPORT. PLEASE REVIEW YOUR SERVICE OR SUBSCRIPTION AGREEMENT(S) THAT YOU MAY HAVE WITH RED HAT OR OTHER AUTHORIZED RED HAT SERVICE PROVIDERS REGARDING SERVICES AND ASSOCIATED PAYMENTS.

This end user license agreement ("EULA") governs the use of any of the versions of Red Hat Enterprise Linux, certain other Red Hat software applications that include or refer to this license, and any related updates, source code, appearance, structure and organization (the "Programs"), regardless of the delivery mechanism.

1. **License Grant.** Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to you a perpetual, worldwide license to the Programs (most of which include multiple software components) pursuant to the GNU General Public License v.2. The license agreement for each software component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (subject to certain obligations in some cases), both in source code and binary code forms, with the exception of (a) certain binary only firmware components and (b) the images identified in Section 2 below. The license rights for the binary only firmware components are located with the components themselves. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms of any particular component.

2. **Intellectual Property Rights.** The Programs and each of their components are owned by Red Hat and other licensors and are protected under copyright law and under other laws as applicable. Title to the Programs and any component, or to any copy, modification, or merged portion shall remain with Red Hat and other licensors, subject to the applicable license. The "Red Hat" trademark and the "Shadowman" logo are registered trademarks of Red Hat in the U.S. and other countries. This EULA does not permit you to distribute the Programs or their components using Red Hat's trademarks, regardless of whether the copy has been modified. You may make a commercial redistribution of the Programs only if (a) permitted under a separate written agreement with Red Hat authorizing such commercial redistribution, or (b) you remove and replace all occurrences of Red Hat trademarks. Modifications to the software may corrupt the Programs. You should read the information found at http://www.redhat.com/about/corporate/trademark/ before distributing a copy of the Programs.

3. **Limited Warranty.** Except as specifically stated in this Section 3, a separate agreement with Red Hat, or a license for a particular component, **to the maximum extent permitted under applicable law, the Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose.** Red Hat warrants that the media on which the Programs and the components are provided will be free from defects in materials and manufacture under normal use for a period of 30 days from the date of delivery to you. Neither Red Hat nor its affiliates warrants that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements. **This warranty extends only to the party that purchases subscription services for the Programs from Red Hat and/or its affiliates or a Red Hat authorized distributor.**

4. **Limitation of Remedies and Liability.** To the maximum extent permitted by applicable law, your exclusive remedy under this EULA is to return any defective media within 30 days of delivery along with a copy of your payment receipt and Red Hat, at its option, will replace it or refund the money you paid for the media. **To the maximum extent permitted under applicable law, under no circumstances will Red Hat, its affiliates, any Red Hat authorized distributor, or the licensor of any component provided to you under this EULA be liable to you for any incidental or consequential damages, including lost profits or lost savings arising out of the use or inability to use the Programs or any component, even if Red Hat, its affiliates, an authorized distributor and/or licensor has been advised of the possibility of such damages. In no event shall Red Hat's or its affiliates' liability, an authorized distributor's liability or the liability of the licensor of a component provided to you under this EULA exceed the amount that you paid to Red Hat for the media under this EULA.**

5. **Export Control.** As required by the laws of the United States and other countries, you represent and warrant that you: (a) understand that the Programs and their components may be subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) are not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, North Korea, Sudan and Syria, subject to change as posted by the United States government); (c) will not export, re-export, or transfer the Programs to any prohibited destination or persons or entities on the U.S. Bureau of Industry and Security Denied Parties List or Entity List, or the U.S. Office of Foreign Assets Control list of Specially Designated Nationals and Blocked Persons, or any similar lists maintained by other countries, without the necessary export license(s) or authorization(s); (d) will not use or transfer the Programs for use in connection with any nuclear, chemical or biological weapons, missile technology, or military end-uses where prohibited by an applicable arms embargo, unless authorized by the relevant government agency by regulation or specific license; (e) understand and agree that if you are in the United States and export or transfers the Programs to eligible end users, you will, to the extent required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry and Security, which include the name and address (including country) of each transferee; and (f) understand that countries including the United States may restrict the import, use, or export of encryption products (which may include the Programs and the components) and agree that you shall be solely responsible for compliance with any such import, use, or export restrictions.

End User License Agreement   Page 1 of 2
Red Hat® Enterprise Linux® and Red Hat Applications   November 2010

6. **Third Party Programs.** Red Hat may distribute third party software programs with the Programs that are not part of the Programs. These third party programs are not required to run the Programs, are provided as a convenience to you, and are subject to their own license terms. The license terms either accompany the third party software programs or can be viewed at http://www.redhat.com/licenses/thirdparty/eula.html. If you do not agree to abide by the applicable license terms for the third party software programs, then you may not install them. If you wish to install the third party software programs on more than one system or transfer the third party software programs to another party, then you must contact the licensor of the applicable third part y software programs.

7. **General.** If any provision of this EULA is held to be unenforceable, the enforceability of the remaining provisions shall not be affected. Any claim, controversy or dispute arising under or relating to this EULA shall be governed by the laws of the State of New York and of the United States, without regard to any conflict of laws provisions. The rights and obligations of the parties to this EULA shall not be governed by the United Nations Convention on the International Sale of Goods.