Contract #: AR3103

STATE OF UTAH COOPERATIVE CONTRACT

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

Global Tech, Inc. dba eGlobalTech
Name

3865 Wilson Blvd., Suite 700
Street Address

Arlington	VA	22203
City	*State*	*Zip*

Vendor # VC226562 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact *Name:* Theresa Grouge *Phone Number:* 571-224-9375 *Email:* Theresa.grouge@eglobaltech.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

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

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

5. CONTRACT PERIOD: Effective Date: Monday, April 01, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

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

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

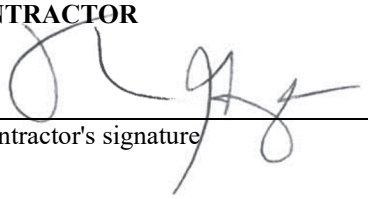
Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

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

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

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

CONTRACTOR



Contractor's signature — Date: 4/4/2019

Theresa Grouge, Director of Contracts
Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes
Christopher Hughes (Apr 9, 2019)

Director, Division of Purchasing — Date: Apr 9, 2019

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason

to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

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

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

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

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

10. Defaults and Remedies

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

(1) Nonperformance of contractual requirements; or

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

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

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

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

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

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

13. Indemnification

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

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

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

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

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

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

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

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

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

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

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

16. Insurance

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

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

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

aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

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

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

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

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

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

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

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

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

19. Ordering

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

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

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

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

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

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

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

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

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

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

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this

authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26. Records Administration and Audit.

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

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

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

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

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its

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

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

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

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

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

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

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

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

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

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

Services it acquires from this Master Agreement.

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

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

32. Transition Assistance:

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

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

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

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

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection

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

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

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

37. Governing Law and Venue

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

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

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

d. This section is also not a waiver by the Participating State of any form of immunity,

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

within the Participating State.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

8. Background Checks:

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

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

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

9. Access to Security Logs and Reports:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Infrastructure as a Service (IaaS)

1.2 Risk Categorization.

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

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
IaaS	Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Elastic Compute Cloud (Amazon EC2)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon EC2 Container Service	Amazon EC2 Container Service	Amazon EC2 Container Service	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Lambda	AWS Lambda	AWS Lambda	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Auto Scaling	AWS Auto Scaling	AWS Auto Scaling	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Elastic Load Balancing	Elastic Load Balancing	Elastic Load Balancing	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Virtual Private Cloud (Amazon VPC)	Amazon Virtual Private Cloud (Amazon VPC)	Amazon Virtual Private Cloud (Amazon VPC)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Route 53	Amazon Route 53	Amazon Route 53	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Direct Connect	AWS Direct Connect	AWS Direct Connect	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3)	Amazon Simple Storage Service (Amazon S3)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Glacier	Amazon Glacier	Amazon Glacier	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Elastic Block Store (Amazon EBS)	Amazon Elastic Block Store (Amazon EBS)	Amazon Elastic Block Store (Amazon EBS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon CloudFront	Amazon CloudFront	Amazon CloudFront	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Import/Export	AWS Import/Export	AWS Import/Export	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Storage Gateway	AWS Storage Gateway	AWS Storage Gateway	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Relational Database Service (Amazon RDS)	Amazon Relational Database Service (Amazon RDS)	Amazon Relational Database Service (Amazon RDS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon DynamoDB	Amazon DynamoDB	Amazon DynamoDB	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Redshift	Amazon Redshift	Amazon Redshift	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon ElastiCache	Amazon ElastiCache	Amazon ElastiCache	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Elastic	Amazon Elastic	Amazon Elastic	Private Cloud, Community Cloud,

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
	MapReduce (Amazon EMR)	MapReduce (Amazon EMR)	MapReduce (Amazon EMR)	Public Cloud, Hybrid Cloud
IaaS	Amazon Kinesis	Amazon Kinesis	Amazon Kinesis	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Data Pipeline	AWS Data Pipeline	AWS Data Pipeline	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Mobile Analytics	Amazon Mobile Analytics	Amazon Mobile Analytics	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Identity and Access Management (IAM)	AWS Identity and Access Management (IAM)	AWS Identity and Access Management (IAM)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Directory Service	AWS Directory Service	AWS Directory Service	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Service Catalog	AWS Service Catalog	AWS Service Catalog	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Config	AWS Config	AWS Config	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CloudHSM	AWS CloudHSM	AWS CloudHSM	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Key Management Service (KMS)	AWS Key Management Service (KMS)	AWS Key Management Service (KMS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CloudTrail	AWS CloudTrail	AWS CloudTrail	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon CloudWatch	Amazon CloudWatch	Amazon CloudWatch	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Management Console	AWS Management Console	AWS Management Console	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Command Line Interface (CLI)	AWS Command Line Interface (CLI)	AWS Command Line Interface (CLI)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	APIs	APIs	APIs	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS Elastic Beanstalk	AWS Elastic Beanstalk	AWS Elastic Beanstalk	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CloudFormation	AWS CloudFormation	AWS CloudFormation	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CodeDeploy	AWS CodeDeploy	AWS CodeDeploy	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CodeCommit	AWS CodeCommit	AWS CodeCommit	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS CodePipeline	AWS CodePipeline	AWS CodePipeline	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	AWS OpsWorks	AWS OpsWorks	AWS OpsWorks	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon WorkDocs	Amazon WorkDocs	Amazon WorkDocs	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon WorkSpaces	Amazon WorkSpaces	Amazon WorkSpaces	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon AppStream	Amazon AppStream	Amazon AppStream	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon CloudSearch	Amazon CloudSearch	Amazon CloudSearch	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Simple Workflow Service (Amazon SWF)	Amazon Simple Workflow Service (Amazon SWF)	Amazon Simple Workflow Service (Amazon SWF)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
IaaS	Amazon Simple Queue Service	Amazon Simple Queue Service	Amazon Simple Queue Service	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
	(Amazon SQS)	(Amazon SQS)	(Amazon SQS)	
laaS	Amazon Simple Email Service (Amazon SES)	Amazon Simple Email Service (Amazon SES)	Amazon Simple Email Service (Amazon SES)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
laaS	Amazon Simple Notification Service (Amazon SNS)	Amazon Simple Notification Service (Amazon SNS)	Amazon Simple Notification Service (Amazon SNS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
laaS	Amazon Elastic Transcoder	Amazon Elastic Transcoder	Amazon Elastic Transcoder	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
laaS	Amazon Cognito	Amazon Cognito	Amazon Cognito	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
laaS	Amazon Flexible Payments Service (Amazon FPS)	Amazon Flexible Payments Service (Amazon FPS)	Amazon Flexible Payments Service (Amazon FPS)	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
laaS	AWS Support	AWS Support	AWS Support	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud
laaS	AWS Trusted Advisor	AWS Trusted Advisor	AWS Trusted Advisor	Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

2.1 Deployment Models.

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

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

Attachment C - Pricing Discounts and Schedule

Contractor: Global Tech, Inc. dba eGlobalTech

Pricing Notes

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

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

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

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

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

Cloud Service Model: Infrastructure as a Service (IaaS)

IaaS Minimum Discount % Off

Description	Discount
IaaS Minimum Discount %*	5.00%

*(applies to all OEM's offered within this service model)

Additional Value Added Services

Item Description		Onsite Hourly Rate		Remote Hourly Rate	
		NVP Price	Catalog Price	NVP Price	Catalog Price
Maintenance Services					
	Cloud Admin I	$77.52	$86.82	$82.42	$92.31
	Cloud Admin II	$100.31	$112.35	$106.65	$119.45
	Help Desk Analyst I	$72.95	$81.70	$77.56	$86.87
	Help Desk Analyst II	$82.07	$91.92	$87.25	$97.72
	Security Analyst	$95.76	$107.25	$101.81	$114.03
Professional Services					
	Deployment Services				
	DevOps Engineer I	$132.23	$148.10	$140.58	$157.45
	DevOps Engineer II	$145.90	$163.41	$155.11	$173.72
	Security Engineer	$141.34	$158.30	$150.28	$168.31
	Integration Services				
	Software Engineer I	$118.55	$132.78	$126.03	$141.15
	Software Engineer II	$150.47	$168.53	$159.96	$179.16
	System Architect	$164.15	$183.85	$174.53	$195.47
	Project Manager	$155.01	$173.61	$164.81	$184.59
	Program Manager	$186.95	$209.38	$198.75	$222.60
	Consulting/Advisory Services				
	Subject Matter Specialist I	$227.96	$255.32	$242.37	$271.45
	Architectural Design Services				
	Cloud Architect I	$127.68	$143.00	$135.74	$152.03
	Cloud Architect II	$173.27	$194.06	$184.22	$206.33
	Security Architect	$162.32	$181.80	$172.58	$193.29
	Statement of Work Services				
	Business Analyst I	$86.63	$97.03	$92.09	$103.14
	Business Analyst II	$113.99	$127.67	$121.20	$135.74
Partner Services					
	Subject Matter Specialist II	$291.81	$326.83	$310.24	$347.47
Training Deployment Services					
	Agile Coach I	$168.71	$188.96	$179.37	$200.89
	Agile Coach II	$200.63	$224.71	$213.30	$238.90
	Cloud Training SME	$255.34	$285.98	$271.47	$304.05

Deliverable Rates	
NVP Price	Catalog Price

Attachment C - Pricing Discounts and Schedule

Contractor: Global Tech, Inc. dba eGlobalTech

N/A	N/A	N/A
N/A	N/A	N/A

NASPO ValuePoint Master Agreement for Cloud Solutions

Technical Response

July 6, 2018

Submitted to:

State of Utah, Division of Purchasing

Attn: Solomon Kingston, State Contract Analyst

3150 State Office Building

Capitol Hill Complex

450 North State Street

Salt Lake City, UT 84114

skingston@utah.gov

(801) 538-3228

Table of Contents

1 Narrative of eGT's Assessment of Cloud Solutions (A)

eGlobalTech (eGT) proposes the adoption and usage of Amazon Web Services (AWS) to fulfill Infrastructure as-a Service (IaaS) cloud requirements of NASPO and the individual participating US States. Using AWS, customers can requisition compute power, storage, network, security and other services in minutes and have the flexibility to choose the development platform or programming model that makes the most sense for the problems they are trying to solve. Customers pay only for what they use, with no upfront expenses or long-term commitments, making AWS a cost-effective way to deliver applications. eGT has proven experience supporting several U.S. Federal agencies including Department of Homeland Security (DHS) and the Department of Health and Human Services (HHS) in providing cloud acquisition and migration services for over six years. We leveraged these experiences to construct DevOps Factory, our cloud-focused services offering composed of high caliber certified cloud engineers and architects. DevOps Factory and AWS are the two primary pillars of our overall approach and solution to meet NASPO's requirements and drive successful cloud adoption at participating US States. In the following sections we further elaborate our overall understanding, approach and capability to fulfill NASPO's cloud requirements.

1.1 eGT's Understanding

The advent of secure cloud computing has opened a strategic opportunity for government institutions to shed their burden in managing or utilizing outdated brick and mortar datacenters and on-premise server hardware to fulfill their IT requirements. State and local organizations now can outsource their computing needs by using such secure cloud platforms and focus on delivering mission-centric IT and digital capabilities. It eliminates the need for huge capital expenditure while enabling them to be leaner and better adapt to changing business needs. The adoption and usage of cloud platforms, however requires proper planning, architecture, and implementation approach that mitigates short and long-term risks such as scalability, performance, and security.

1.2 eGT's Ability and Overall Approach

eGT has unique experience migrating and implementing mission critical applications on multiple cloud platforms including AWS, Azure and Google Cloud Platform for numerous federal agencies including the DHS, the HHS, the Department of Education (DoED) and the Environmental Protection Agency (EPA). AWS certified eGT as an Advanced Consulting Partner (ACP) and "Public Sector Partner" attesting to our deep expertise in AWS and recognizing the growing contingent of AWS certified cloud engineers and architects under our employment.

Through these years of experience, we have matured our overall approach to migration, implementation and operations of cloud based solutions. eGT's DevOps Factory framework illustrated in **Figure 1** informs our overall approach to implementing cloud based solutions. DevOps Factory has been matured through several years of leading DevOps initiatives in federal government and commercial institutions, focuses on accelerating delivery of secure functional software through innovative streamlined automation. DevOps Factory leverages best of breed commercial and open source technologies such as Chef and Jenkins to instrument a CI/CD pipeline automating all repetitive tasks including security compliance tests, cloud deployments,

and Operations and Maintenance (O&M) tasks. DevOps Factory also includes tools developed by eGT Labs, such as Cloudamatic (https://www.cloudamatic.com), a full stack orchestration framework that automates the provisioning, configuration, orchestration, and post-deployment management of complex multi-tier architectures. Cloudamatic is 100% open source, available through Berkley Software Distribution (BSD) license and free for government use.

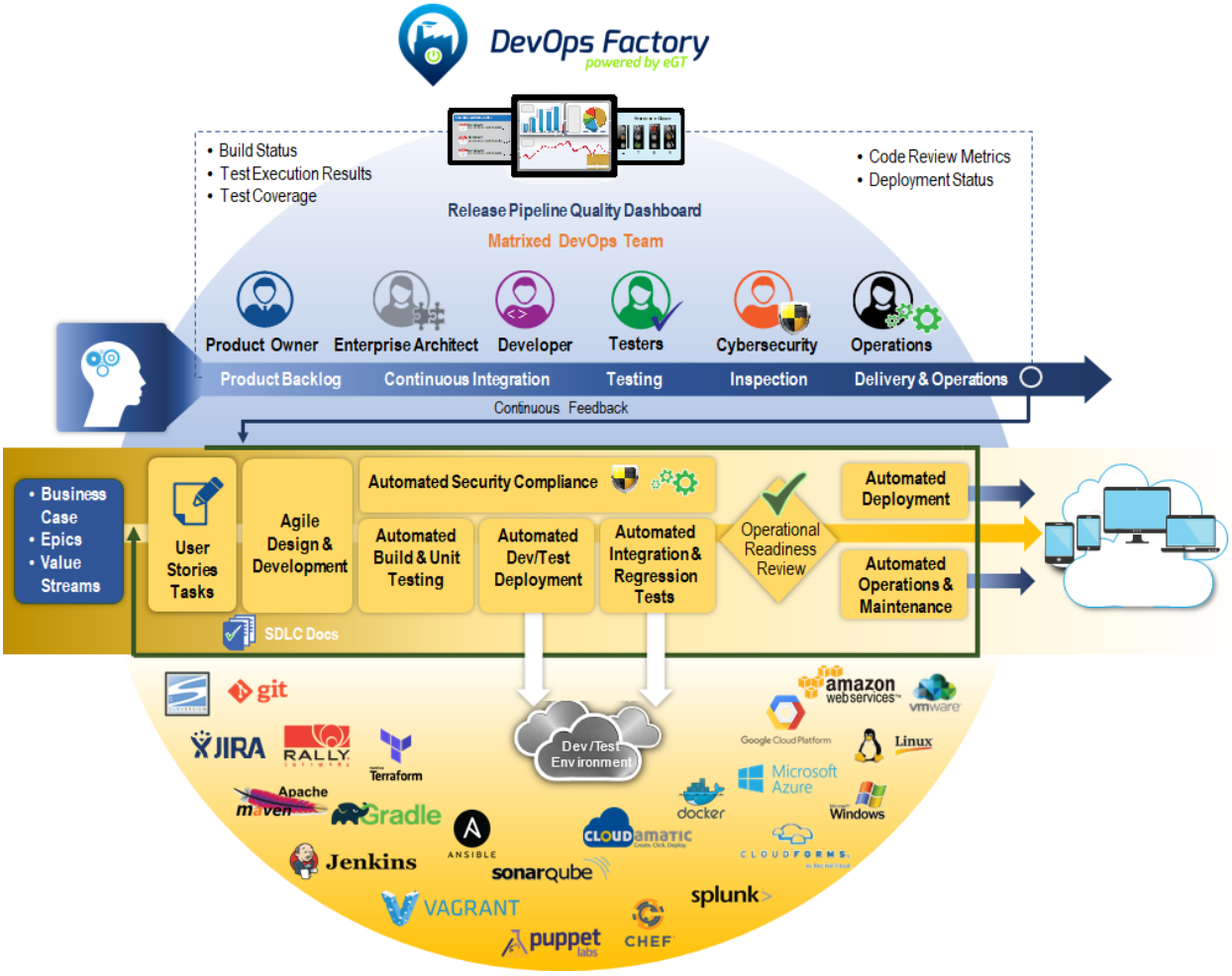


Figure 1 | eGT configures the DevOps Factory cloud migration framework with tools most effective to each customer and system

Our mature cloud solutions combined with our proven past performances and highly experienced staff of cloud engineers, is well positioned to support NASPO and the participating states in their cloud migration and implementation initiatives.

1.3 Resources to Fulfill the Requirements

eGT has a highly diverse technical staff ranging from specialized technologists, full stack developers, cloud architects, security engineers and advanced DevOps engineers. Our engineers are active contributors to open source community projects producing next generation automation tools, technologies and practices. In the following table we highlight a few of our key technical staff members and their capabilities and qualifications.

DevOps Community Involvement. In July 2016, 2017, and 2018, eGT staff exhibited and spoke at the DevOpsDays DC Conference (www.devopsdays.org).

eGT Employee	Capabilities and Qualifications
Todd Baylor	20+ years of experience leading IT development teams delivering commercial products and Federal systems. Certified AWS Solutions Architect - Associate
Rajiv Kadayam	18+ years of experience driving new software product development and modernization initiatives at both government and commercial organizations including DHS, FEMA, HHS, USPTO, GSA, CMS, Department of Labor (DOL), and IBM. Active speaker at technical conferences including DevOpsDays DC and ISACA. Certified Scrum Master (CSM) leading multiple agile projects in eGT Labs.
Robert Patt-Corner	Principal Architect, designer, and development team leader focusing on cloud computing, systems modernization, and DevOps. Holds multiple AWS professional and IBM certifications. Co-inventor of Cloudamatic.
John Stange	18+ years of experience and a lead DevOps engineer supporting several cloud migration and enablement projects at FEMA, HHS, FlatWorld, National Institutes of Health (NIH), DoED, and EPA. Co-inventor and lead committer of Cloudamatic open source project. Holds AWS Solutions Architect Professional and Acquia Certified Drupal Developer certifications.
Zach Rowe	8+ years of experience as a Senior Consultant and DevOps engineer, currently supporting FEMA's mission critical DMSE Cloud and projects at HHS. Holds AWS Solutions Architect Professional certification and actively contributes to Cloudamatic open source project.
Ryan Bolyard	DevOps engineer with strong foundational experience with Chef and Web CMS platforms. Currently possesses Chef Fluency Badge and AWS Solutions Architect - Associate
Clara Bridges	Full Stack Developer and Polyglot with deep expertise in Java, Node.JS, Python, Ruby, and React.JS. Strong track record of developing innovative single page web applications for both federal and commercial clients.
Eric Hanson	Principal Technical Lead and hands-on Full Stack Developer with proven track record of building robust enterprise applications and systems for USPTO and Federal Communications Commission (FCC). Deep expertise in multiple programming languages including Java, Scala, Node.JS, Angular.JS and React.JS.
Manasa Pandurangi	Full Stack Developer with proven track record of building high performance modern applications using Java, SpringBoot, MongoDB, and Angular.JS for HHS. Equally adept in Scala and Node.JS and was a key contributor to a computation engine for a data analytics application for GSA.

1.4 Proposed Options or Alternatives

eGT is proposing no additional options or alternatives to the solution and approach we have provided.

2 Technical Requirements (B) (8.1)

AWS is a leader in cloud computing, providing services to the Federal Government as well as the Fortune 100. AWS systems meet all five, essential requirements of cloud computing and offer leading IaaS and PaaS cloud services and solutions needed to meet customer needs.

eGT is an AWS ACP for the public-sector and an ACP authorized government reseller. Achieving this status requires a deep understanding of the architecture and features of the system and ensures that eGT has the personnel and expertise needed to assist customers with selecting and implementing cloud solutions. eGT is one of the few companies that can combine agility and personalized customer service with a deep technical expertise.

2.1 Meeting the NIST Essential Characteristics (8.1.1)

The National Institute of Standards and Technology (NIST) defines cloud computing in NIST Special Publication 800-145. Cloud computing is defined as "…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This model for computing is defined by five essential characteristics including:

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

On-Demand Self-Service. AWS provides customers with multiple options for on-demand access to a wide range of cloud-based services, such as virtual machines, compute capabilities, networking, databases, storage, analytics, mobile, developer tools, security and enterprise applications that customers provision on-demand through their AWS portal. AWS enables customers to eliminate the need for costly hardware and the administrative pain that goes along with owning and operating it

As an example, AWS customers and can immediately begin deployment in the cloud with the equivalent of 1, 10, 100, or 1,000 servers with a customer designated level for performance and memory needed to fit their requirements. eGT was able to seamlessly scale to support 400% growth in usage of services on the FEMA Disaster Management Support Environment (DMSE) Cloud with little or no impact to performance.

Broad Network Access. Customers access a wide range of AWS services through a web-based application or portal via the internet. These applications or internet portals provide access to AWS access servers, storage, databases, and a broad set of application services and satisfying the requirement for broad network access. AWS owns and maintains the network-connected hardware required for these application services, which are then provisioned by the customer via the internet.

Resource Pooling. Resource pooling is usually implemented through virtualization, which allows hardware resources, such as processing, memory and storage, to be divided to serve the needs of multiple tenants within the cloud system. AWS implements security management

processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and complies with all requirements of PCI DSS Security Standards 3.2 as of July 2016.

Rapid Elasticity. Within a cloud environment, rapid elasticity means that the system can instantly scale to meet the demand of its customers. AWS is able to quickly scale by providing a massive global cloud infrastructure that can provide servers that scale up or scale down as needed. NASPO can be confident that their existing infrastructure can handle a spike in traffic without interfering with normal business operations. Elastic Load Balancing and Auto Scaling can automatically scale a customer's AWS resources up to meet unexpected demand and then scale those resources down as demand decreases.

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

2.2 Attachment C and Attachment D (8.1.2 & 8.1.3)

Attachment C: NIST Service Models

eGT offers AWS' deep catalog of services provided using the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) service models. A description of the AWS IaaS, and PaaS services are provided below, along with the service sub category and descriptor.

Infrastructure as Service Offerings (IaaS):

NIST defines IaaS as providing services to the customer that allow for the provisioning of fundamental computing resources (processing, storage, networking, etc.) where the customer can deploy and run operating systems or applications without controlling the underlying cloud infrastructure.

eGT can offer core AWS IaaS offerings, such as compute (virtual machines), networking services and storage. These service offering are viewed as the gold standing for IaaS cloud across the industry.

(IaaS) Subcategory	Descriptor
Computer/Infrastructure Services	Virtual Machines
Internet of Things	Operating System
Network	Content Delivery Networks (CDNs) Direct Link DNS Firewall Gateway Inventory Tool Load balancer Virtual Network
Security	DDOS Monitoring/Management Identity & Access Management Key Management Network Security
Storage	Archive Block CDNs File Object

Platform as a Service (PaaS) Offerings:

NIST defines PaaS as the ability to allow customer to deploy applications created using programming languages, libraries, services, and tools supported by the provider into cloud infrastructure. However, the consumer does not manage or control the underlying cloud infrastructure but may have some control over the deployed applications including configuration settings for the application-hosting environment.

eGT offers class leading, AWS PaaS, allowing customers to quickly move and deploy into the cloud. AWS offers a range of PaaS providing customers with the option to use a PaaS that does allow more granular control of configurations and resources to managed PaaS services that automate those tasks.

(PaaS) Subcategory	Descriptor
Analytics	Business Intelligence Data Warehouse Extract, Transform, and Load (ETL) service Hadoop Interactive Query Service Real-time Video Analytics Search Service
Database	Data Warehouse Database Migration Service Graph Database In-Memory Data Store NoSQL Relational

(PaaS) Subcategory	Descriptor
Development, Testing and Deployment	Managed Build Service Application/Virtual Machine Migration Automated Deployment Service Batch Management Code/Application Repository Containers Deployment Automation Hybrid compute, storage, and networking platform Internet of Things Internet of Things Runtime Environments Tool
Integration (iPaaS)	Application Integration Messaging/Notification Service Hybrid Storage Server/Machine Migration VMWare Cloud Message Broker
Security	Application Scanner Identity & Access Management Internet of Things Data Transport Solution

Attachment D: Scope of Services

Cloud Based Service Providers:

AWS meets the NIST guidance for essential characteristics of cloud and offers a deep catalog of leading cloud computing services to meet customer requirements. AWS' NIST compliant cloud infrastructure services have been validated by third-party testing performed against the NIST 800-53 Rev. 4 controls plus FedRAMP requirements. AWS has received FedRAMP Authorizations to Operate (ATO) from multiple authorizing agencies for both the AWS GovCloud (US) Region and the AWS US East/West regions. AWS' whitepaper NIST Cybersecurity Framework (CSF) Aligning to the NIST CSF in the AWS Cloud evaluates the NIST CSF and the many AWS Cloud offerings public and commercial sector customers can use to align to the NIST CSF to improve your cybersecurity posture. It also provides a third-party auditor letter validating attestation confirming AWS services' conformance to the NIST CSF risk management practices, allowing you to properly protect your data across AWS.

AWS' alignment with the NIST framework means that as customers build systems and applications on AWS some controls are specifically inherited from AWS and many of the controls have shared inheritance between the customer and AWS. Under NDA, AWS provides an AWS FedRAMP SSP template based upon NIST 800-53 Rev. 4, which is pre-populated with the applicable NIST 800-5 Rev. 4 low/moderate/high control baseline.

Categorization of Risk:

eGT is able offer AWS cloud-based services that have been assessed and categorized for the risk impact level of the data that is able to be stored within the system in line with the guidance of FIPS Publication 199 “Standards for Security Categorization of Federal Information and Information Systems. AWS East/West can process and store data at the moderate impact level and AWS GovCloud is able to process and store high impact data.

eGT is also mindful that in the IaaS and PaaS service models, customers share responsibility to secure their applications and will need to perform their own impact assessment of data that they plan to put into the cloud. eGT offers the expertise needed to assist customers in identifying controls that are either shared or their responsibility and using FIPS 199 to assess the risk level of the data they intend to out into the cloud. This will also help customers select the proper environment to ensure the security of their data.

Services and Models:

As demonstrated in section 2.1, eGT can offer AWS cloud services that meet the NIST SP 800-145 definition of the five essential cloud computing characteristics of On-Demand Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity, and Measured Service.

AWS offers a deep catalog of market leading cloud service IaaS and PaaS Services. A partial list of available AWS, available through eGT is listed below:

IaaS Services:

- Amazon EC2 - Virtual Servers in the Cloud
- Amazon VPC - Isolated Cloud Resources
- Amazon CloudFront - Global Content Delivery Network
- Amazon Route 53 - Scalable Domain Name System
- Elastic Load Balancing - High Scale Load Balancing
- AWS Identity & Access Management - Manage User Access and Encryption Keys
- AWS Directory Service - Host and Manage Active Directory
- AWS Key Management Service - Managed Creation and Control of Encryption Keys
- AWS Shield - DDoS Protection
- Amazon S3 - Scalable Storage in the Cloud
- Amazon Elastic File System - Managed File Storage for EC2

PaaS Services:

- Amazon Athena - Query Data in S3 using SQL
- Amazon Elasticsearch Service - Run and Scale Elasticsearch Clusters
- Amazon EMR - Hosted Hadoop Framework
- Amazon Quicksight - Fast Business Analytics Service
- AWS Data Pipeline - Orchestration Service for Periodic, Data-driven Workflows
- Amazon Aurora - High Performance Managed Relational Database
- Amazon RDS - Managed Relational Database Service for MySQL, PostgreSQL, Oracle, SQL Server, and MariaDB
- Amazon DynamoDB - Managed NoSQL Database
- Amazon Redshift - Fast, Simple, Cost-effective Data Warehousing

- Amazon Neptune - Fully Managed Graph Database Service
- AWS Database Migration Service - Migrate Databases with Minimal Downtime
- Amazon Elastic Container Service (Amazon ECS) for Kubernetes - Run Managed Kubernetes on AWS
- Amazon Elastic Container Registry -Store and Retrieve Docker Images
- AWS Elastic Beanstalk - Run and Manage Web Apps
- AWS CodeStar - Develop and Deploy AWS Applications
- AWS CodeCommit - Store Code in Private Git Repositories
- AWS X-Ray - Analyze and Debug Your Applications
- AWS IoT Core - Connect Devices to the Cloud
- VMware Cloud on AWS - Build a Hybrid Cloud without Custom Hardware
- AWS Snowmobile - Exabyte-scale Data Transport
- AWS cloud services are provided through Public Cloud, Community Cloud (Government Community Cloud), and Hybrid Cloud deployment models.

Public Cloud

AWS East/West meets the NIST definition for public cloud as the cloud service and open for use by the general public and the cloud infrastructure exists on premises of the cloud provider.

Community Cloud

AWS GovCloud meets the definition of a community cloud as AWS GovCloud is provisioned for exclusive use by a specific community of consumers. In this case GovCloud is an AWS region designed to address specific regulatory and compliance requirements of U.S. government agencies at the federal, state, and local level, as well as contractors, educational institutions, and other US customers that run sensitive workloads in the cloud.

Hybrid Cloud

AWS Hybrid Cloud solutions meet the NIST deployment model definition by connecting two or more distinct infrastructures, binding them together by standardized or proprietary technology that enables data and application portability.

A hybrid cloud environment allows organizations to address immediate IT needs though utilizing the benefits of cloud computing, while also retaining on-premises infrastructure. A hybrid model is a prudent approach to cloud adoption for organizations that require the immediate use of scalable cloud services but are not ready to fully migrate all application and workloads to the cloud.

AWS provides the tools and solutions to integrate existing on-premises resources with the AWS cloud. By using AWS to enhance and extend your capabilities, without giving up the investments you have already made, you can accelerate your adoption of cloud computing.

AWS Capabilities for Hybrid Cloud Solutions: AWS provides all the capabilities required for a dynamic, reliable, and secure hybrid cloud solution:

Extend Network Configuration: Flexible network connectivity is a cornerstone of integrating distributed environments, including AWS and your existing on-premises equipment. With Amazon VPC, you can extend your on-premises network configuration into your virtual private networks on the AWS cloud. AWS resources can operate as if they are part of your existing

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

Integrated Cloud Backups: AWS helps simplify the backup and recovery environment for the enterprise. You can leverage the on-demand nature of the cloud and automate your backup and recovery processes, so they are not only less complex and lightweight, but also easy to manage and maintain. Storage services with AWS are designed to provide 99.999999999% durability, so you can feel confident your backups are protected.

Integrated Network Connection: On-premises connection with AWS is best accomplished with AWS Storage Gateway, a software appliance installed in your data center with cloud-based storage to provide seamless and secure integration between an organization's existing IT environment and the AWS storage infrastructure. Using industry-standard storage protocols, the service allows you to store data in the AWS cloud for scalable and cost-effective storage. It provides low-latency performance by maintaining frequently accessed data on-premises while securely storing all your data encrypted in the Amazon Simple Storage Service (Amazon S3) or Amazon Glacier.

Integrated Resource Management and Workload Migration: All AWS cloud services are driven by robust APIs that allow for a wide variety of monitoring and management tools that integrate easily with your AWS cloud resources. It's likely that many of the tools that your organization is using to manage your on-premises environments can be extended to include AWS as well. Integrating your AWS environment can provide a simpler and quicker path for cloud adoption, because your operations team does not need to learn new tools or develop completely new processes.

3 Subcontractors (8.2)

eGT is an AWS Channel Reseller and is a member of the AWS Government Partner Program. The firm has a large contingent of AWS certified engineers as well as experienced staff in a broad range of business and technology areas, which continues to grow each year. eGT is capable of not only selling AWS services but also independently provide the required assessment, implementation, and transition services for a complete end-to-end solution with no additional support from sub-contractors. We currently provide Cloud consulting resources to numerous government clients including the National Institutes of Health (NIH), HHS, DHS and the Federal General Services Administration (GSA) where eGT provided PMO support for the Federal Risk and Authorization Management Program (FedRAMP) Management Program. Our intent is to not use sub-contractors in the execution of this contract, unless otherwise recommended by a customer or purchasing entity to improve the probability of successful project completion.

3.1 Plan for Providing Services (8.2.1)

eGT intends to provide all services without the requirement of sub-contractors.

3.1.1 Subcontractor Fulfillment of RFP Requirements (if applicable)

eGT does not intend to use subcontractors in the execution of this contract. In the unlikely event we do require the use of a subcontractor, they will meet all the Administrative, Business and Technical requirements of the RFP.

3.2 Extent of Subcontractor Use (8.2.2)

eGT does not intend to use subcontractors for this engagement. In the unlikely event eGT does require the use of a subcontractor, their use will be minimal and focused on areas in which special skills are required.

3.2.1 Subcontractor Involvement

eGT does not intend to use subcontractors for this engagement. In the unlikely event eGT does require the use of a subcontractor, their use will be minimal and focused on areas in which special skills are required.

3.3 Subcontractor Qualifications (8.2.3)

eGT does not intend to use subcontracts in the execution of this contract.

3.3.1 Subcontractor Selection

eGT does not intend to use subcontracts in the execution of this contract. However, in the event a special skill is required where a subcontractor is needed, eGT will attempt to use only firms known and previously used on similar engagements in the past. eGT maintains a set of firms that not only augments our own capabilities but also that are trusted partners, having been engaged on eGT efforts in the past. These firms capabilities span a broad range of business and technical skills and expertise.

Many of these firms are small businesses, woman owned, veteran owned, disadvantaged (e.g., 8(a)), and/or hub zone. eGT is willing and capable of providing subcontractors with any of the above business classifications to meet any specific task order requirements.

3.3.2 Ensuring Subcontractors Meet all SOW Requirements

In the unlikely event that eGT requires the use of a subcontractor, we will enter into a formal subcontract agreement with the firm. This subcontract will include a copy of the SOW and all terms and conditions of this contract with specific language that all requirements “flow down” to the subcontractor. In addition, subcontractors will be monitored by eGT including their adherence to all contract requirements. In the event of any deficiencies, eGT will either engage the subcontractor in a resolution plan or will terminate the subcontract, either performing this work ourselves or engaging a new subcontractor.

4 Working with Purchasing Entities (8.3)

eGT has extensive experience providing managed cloud services to government institutions that involves handling and securing sensitive personally identifiable information (PII) data. Below we highlight our approach to working with Purchasing Entities in a wide variety of requirements as laid out by NASPO in the RFP.

4.1 Working with Purchasing Entities Before, During, and After Data Breaches (8.3.1)

During a data breach, the Contract Manager will ensure that the required eGT and AWS are applied as appropriate within the requirements of the contract, to support effective and efficient mitigation and response activities. Before a data breach occurs, eGT will review NASPO incident response plans, policies and procedures to understand the roles and responsibilities of stakeholders in the incident response process. Additionally, eGT will ensure that all dependencies within our scope of responsibility are in place to support effective monitoring of the NASPO AWS operating environment.

AWS has implemented a formal, documented incident response policy and program. eGT will comply with this policy which addresses purpose, scope, roles, responsibilities, and management commitment and has been developed in alignment with the ISO 27001 standards, system utilities are appropriately restricted and monitored.

Below is an outline of the three-phased approach AWS has implemented to manage incidents:

1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including:
    a. Metrics and alarms – AWS maintains an exceptional situational awareness capability; most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. Most incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers.
    b. Trouble ticket entered by an AWS employee.
    c. Calls to the 24X7X365 technical support hotline – If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g., Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.
2. Recovery Phase – The relevant resolvers will perform break fix to address the incident. Once troubleshooting, break fix, and affected components are addressed, the call leader will assign next steps in terms of follow -up documentation and follow-up actions and end the call engagement.
3. Reconstitution Phase – Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep-root-cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions, such as design changes etc., will be captured in a Correction of Errors (COE) document and tracked to completion.

In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" (http://status.aws.amazon.com/) is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

The AWS incident management program is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP (both high and moderate) compliance. Additionally, the AWS incident response playbooks are maintained and updated to reflect emerging risks and lessons learned from past incidents. Plans are tested and updated through the due course of business on monthly basis.

4.2 Unauthorized Marketing (8.3.2)

eGT and AWS do not market or sell the Participating Entity's information nor does it allow for any adware, software, or marketing material in its content. eGT employs standard data center security best practices to block adware, malware, and other unwanted intrusions.

4.3 User Test/Staging Environment (8.3.3)

eGT will leverage Amazon ECS, AWS Cloud Formation with infrastructure as code practices and our past Federal contract experience in maintaining different Cloud based environments such as development, testing and staging that are identical to existing production environment. Through Amazon ECS which is a highly scalable, fast, container management service we will manage application-hosting environments on a serverless infrastructure.

These environments will be created, configured, version controlled, maintained and scaled by the software without any human intervention thus providing better integration with development, CI/CD, management tools resulting in greater degree of flexibility, success and meeting urgent demands on a need basis. We will also apply our proven eGT's stage gate review processes with established acceptance criteria to ensure code are moved from application-hosting environment to testing, staging and into production thus resulting in the following benefits:

1. High efficiency and continuous delivery workflow
2. Early identification of defects/pre-emptive discovery of issues
3. Shorter dev/testing life cycles
4. Improved Quality of testing and data integrity
5. Improved Defect Fix Retest Rate
6. Reduced Defect Density in higher environments
7. Quick code turn-around to production

4.4 Accessibility (8.3.4)

In 1990, the U.S. Congress signed into law the Americans with Disability Act to prohibit discrimination against individuals with disabilities in all areas of public life, including jobs, schools, transportation. Under Title I of the American with Disabilities Act, people with disabilities must have access to the same employment opportunities and benefits available to people without disabilities. Employers must also provide reasonable accommodations to qualified applicants or employees.

In 1998, the U.S. Congress amended the Rehabilitation Act of 1973 to require federal agencies to make their electronic and information technology accessible to people with disabilities. Under Section 508, agencies must give disabled employees and members of the public access to information that is comparable to access available to others.

eGT is committed to complying with ADA by ensuring reasonable accommodations requests are provided to qualified applicants or employees. eGT also has over six years of experience developing solutions to the federal government that comply with Section 508 requirements.

eGT will leverage AWS's ElasticWolf Client Console as alternative way for people with disabilities to manage AWS cloud services. ElasticWolf Console is a client-side application with an easy-to-use graphical interface and has been tested for compliance with Section 508 of the Rehabilitation Act. eGT has attached a Voluntary Product Accessibility Template (VPAT) for the ElasticWolf Client Console. This VPAT shows how ElasticWolf Console complies with accessibility standards of the Section 508 of the Rehabilitation Act. AWS's API-based cloud computing services also offer multiple interfaces for its cloud services, including:

- SDKs
- IDE Toolkits
- Command Line Tools

4.5 Browser Platforms (8.3.5)

AWS Management Console supports the following browser platforms.

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

4.6 Working and Cooperating with the Purchasing Entity (8.3.6)

eGT understands the importance of using best practices and government sanctioned business processes. It is what sets a good cooperative procurement apart from others. eGlobal will continue to adhere to these policies and guidelines to ensure that any sensitive or personal information is safe guarded on these state led-contracts.

Prior to the execution of an SLA, eGT will 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 eGT that is subject to any law, rule, or regulation providing for specific compliance obligations.

4.7 Project Schedule/Work Plan (8.3.7)

eGT will utilize our award winning proprietary Project Management Methodology (PMM) Framework as illustrated in **Figure 2**, to derive robust project schedule and work plans.

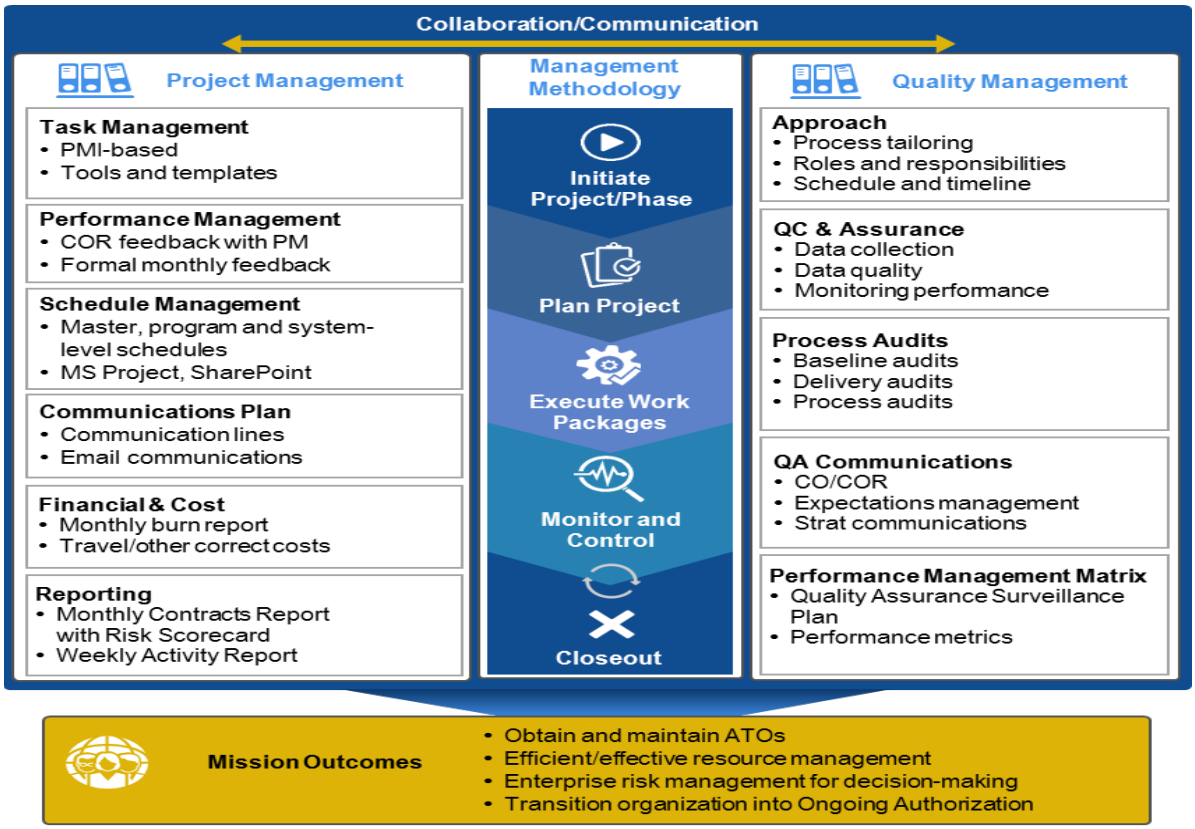


Figure 2 | eGT's PMM drives the successful execution of 40+ federal contracts

eGT will work with Purchasing Entities during the planning phase to identify, optimize and implement Schedule Management process for the management of project schedule/timeline related to development, testing and implementation of solutions for customers. We will leverage Scrum/Kanban methodologies to create an overall integrated project schedule that provides Purchasing Entities a high-level roadmap of project schedule plans.

We will also include Purchasing Entities participation into the scheduling process that will ensure continuous feedback loop mechanism on adjusting the project schedule and work plans in an Agile compatible environment. We will develop a Schedule Management plan in conjunction with the Project Management plan which will describe how the project schedule will be established and managed.

eGT scheduling approach includes a rigorous Work Breakdown Structure (WBS) that decompose and organizes the project to the lowest possible point at which a meaningful and measurable level of effort can be assigned to the activities that are necessary for successful outcomes. It leverages Microsoft Project software tool that runs on Cloud and integrates the project schedule, deliverables, milestones, time, scope and resources required for successful delivery of solutions for customers. This ensures visibility, traceability and accountability of project schedule/work plans to all relevant stakeholders.

4.8 Keeping Up with Technology Changes (8.3.8)

Innovation is a core component of eGT's culture that permeates in every part of our organization including consulting teams working on projects and corporate business operations. eGT Labs, a corporate sponsored Research and Development (R&D) arm, is focused on incubating high-value, reusable solutions, industry partnerships, and thought leadership. eGT clients, through project contracts, can utilize eGT Labs as a platform to experiment and evaluate new products, tools and solutions. We use this platform to stay abreast with the latest and upcoming technologies and practices. eGT is also active in the technology community by attending and speaking at events including DevOps Days DC, AWS Public Sector Summit, Microsoft Azure Government DC, Cloud DC Meetup group, and many others.

4.8.1 Updating Services and Transition Support

eGT and its partner AWS will ensure Service Line Additions and Updates meet requirements outlined in Section 2.12, including Solution service updates and discounts.

An assessment will be conducted by eGT of new AWS services before they are introduced. During the assessment, eGT will first ensure new AWS services meet minimum specifications and term conditions outlined in the Master Agreement and response to the solicitation. The assessment will then provide recommendations on which new AWS services will be introduced. Transition support will be provided by eGT to any Purchasing Entity whose operations are impacted by new services introduced.

AWS provides regular updates on AWS discounts to its partner eGT. These updates help eGT maintain discounts on AWS services. Example updates include:

- Pricing changes and cost reductions of AWS services
- AWS Promotional Credit offers

AWS also provides Simple Monthly Calculator - (https://calculator.s3.amazonaws.com/index.html) to help its customer reduce costs. Simple Monthly Calculator is a tool that allows customers to estimate usage charges for AWS services. eGT will use this tool and discounts offered by AWS to help maintain discounts at the levels set forth in the contract.

5 Customer Service (8.4)

eGT partners with AWS to ensure personalized customer service in real-time. Depending on the issue, the team will provide the right resource(s) to support success. Based on current or planned use cases, the team will also provide a unique combination of tools and expertise to help develop solutions. eGT recognizes the significance and importance of customer data and works adamantly to provide seamless service.

5.1 Ensuring Excellent Customer Service (8.4.1)

eGT will provide excellent customer service to the Purchasing Entities by establishing proper quality assurance measures, developing an Escalation Plan for addressing problems and/or complaints, and adhering to the SLA.

Quality Assurance

eGT's support channel—AWS Support—is a one-on-one, fast response support channel that is staffed 24x7x365 by experienced technical support engineers to provide quality assurance in service areas. This service helps customers of all sizes and technical abilities to successfully use the products and features provided by AWS. The support channel provides a highly personalized level of quality service for customers seeking technical help. Customers who do not choose AWS Support will continue to have access to Basic Support offered at no additional charge. All plans, including Basic Support, provide 24x7 access to customer service, AWS Documentation, Resource Center, Product FAQs, Discussion Forums, and support for Health Checks. All customers with an AWS account will receive Basic Support. To provide the best technical support, eGT offers plans that fit a customer's unique needs.

Customers can contact the support channel through the Support Center. All developer-level support customers can open a case online with "Web Support" using a web browser. Business- and enterprise-level customers have the option to "Click to Call," where an AWS engineer contacts them at a convenient phone number. Enterprise-level customers have a direct access to their dedicated Technical Account Manager (TAM).

Business and enterprise-level customers can also connect to an engineer via Chat. Chat is another way to contact Support. By clicking on the chat support icon in the Support Center, a chat session will be initiated through the browser. This provides real-time, one-on-one interaction with our support engineers and allows additional information and links to be shared for faster issue resolution.

	Basic	Developer	Business	Enterprise
Customer Service – 24x7x365	✓	✓	✓	✓
Support Forums	✓	✓	✓	✓
Documentation, Whitepapers, Best Practice Guides	✓	✓	✓	✓
Access to Technical Support	Support for Health Checks	Email (local business hours)	Phone, Chat, Email (24/7)	Phone, Chat, Email, TAM (24/7)

	Basic	Developer	Business	Enterprise
Primary Case Handling	Technical Customer Service Associate	Cloud Support Associate	Cloud Support Engineer	Sr. Cloud Support Engineer
Users Who Can Create Technical Support Cases		1	Unlimited (AWS Identity and Access Management [IAM] supported)	Unlimited (IAM supported)
Response Time		General guidance: < 24 business hours System impaired: < 12 business hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes
Architecture Support		General Guidance	Contextual Use Case Guidance	Contextual Application Architecture Guidance
Access to Support API			✓	✓
Third-Party Software Support			✓	✓
AWS Trusted Advisor	4 core checks	4 core checks	Full checks	Full checks
Infrastructure Event Management			Contact Us for Pricing	✓
Direct Access to TAM				✓
Architectural Review				✓
Support Concierge				✓
Training				Access to online self-paced labs
Operations Support				Operational reviews, recommendations, and reporting

Escalation Plan

In the event a solution cannot be developed in real-time, the support channel will develop an Escalation Plan for addressing complicated problems or complaints.

Service Level Agreement (SLA)

eGT will ensure its customer service delivery meets the expectations outlined in the SLA between the Purchasing Entities and eGT.

5.2 Compliance with Customer Service Requirements (8.4.2)

eGT will work to comply with customer service requirements respectively for each criterion to ensure customer satisfaction along with metrics submitted with recurring status reports. Metrics would include service and incident response and resolution times as well as customer satisfaction surveys.

5.2.1 Lead Representative (a)

eGT will designate Mr. Todd Baylor as the lead representative. Mr. Baylor comes with 20+ years of experience leading IT development teams delivering commercial products and Federal systems. His experience includes his support to FEMA where he led a large cloud migration projects to the AWS GovCloud platform. He is a certified AWS Solutions Architect – Associate. He will work the COR and PM's on a regular basis via scheduled recurring meetings to ensure that the requirements are on track and satisfaction is met for each participating addendum.

5.2.2 Customer Service Representative Availability and Response time (b & c)

eGT support staff will be available by phone or email (please reference section 11.2 for SLAs. AWS Customer Service Representatives are available 24x7x365 in which multiple forms of contact are provided from its support center portal, which includes a web-based form submission, "click to call" feature and a web-based chat feature. Customer Service Representatives will respond based on the severity of the case in which general inquiries have an SLA of 24 hours and critical or systems down cases have an SLA of 15 minutes or based on the level of support procured from AWS. The level of support procured from AWS can be modified as needed. The Lead Representative along with the Program Manager will provide Quality Assurance measures in the form of predefined SLA's to the purchasing entities.

5.2.3 Design Services (d)

eGT has excellent experience and past performances in providing design services for Cloud Architecture using multiple frameworks and explicitly using the AWS framework. In our support to FEMA, we supported the migration of mission critical disaster response and recovery systems from the DHS data centers to AWS GovCloud platform which required the overall design of the architecture in the form of high level as well as detailed diagrams using MS Visio. All design artifacts will be included in the overall detailed design guide that will illustrate and articulate the design that will be implemented based on NASPO approval and acceptance. For each applicable category, eGT will provide design services and support to meet the requirements.

5.2.4 Installation Services (e)

eGT will provide installation services and support to meet the requirements for each applicable category. As an authorized AWS reseller, eGT provides temporary and long-term cloud services needed to migrate applications to cloud platforms. As one of the few firms of our size to be recognized as an AWS ACP, we have proven delivery capabilities and a close working relationship with the industry's leading CSPs. Prior to any installation as well as implementation services, we will ensure a documented and approved action plan is developed which will coincide with the above-mentioned design guide. Our Lead Representative will ensure that the action plan stays on track and report properly on statuses.

6 Security of Information (8.5)

As an ACP offering AWS cloud services and an AFAQ ISO 27001 Information Security certified organization, eGT understands how important it is to protect customer data and ensure compliance with privacy and security regulations. eGT has put processes and policies in place to ensure the security of customer data. Maintaining the security of customer data and most importantly the trust of the customer is our key goal. eGT also offers AWS services which feature world class security, services and tools used to protect customer data. In addition, AWS services are continuously assessed to meet multiple compliance standards. AWS meets the requirements of the FedRAMP, System and Organization Controls (SOCs) 1, SOC 2, and SOC 3, Payment Card Industry Data Security Standard (PCI DSS), and International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001.

6.1 Data Protection Measures (8.5.1)

Both eGT and AWS implement multiple measures and policies to hold, protect and dispose of customer data.

Acquisition of Customer Data:

eGT does not acquire personal data or non-public personal data (e.g., Personally Identifiable Information, PII) during its work. eGT will only require very limited data from the customer for the purposes of procuring, provisioning and configuring cloud services; providing support; or for the purposes of billing. eGT does not acquire or maintain collections of customer data for any other purpose.

Data Ownership:

Customers of AWS services retain ownership and control over their content within the AWS environment. However, in an IaaS and PaaS environment, the customer also retains responsibility as part of the AWS “shared responsibility” model. While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. As an ACP, eGT can provide customers with the services and best practices to ensure the security of their data within their AWS environment.

While the customer may provide some data to eGT to facilitate the support, operations or provisioning of cloud services, all customer data provided to eGT is owned by the customer. eGT does not claim ownership of any customer provided data or content hosted within the customer’s environment on AWS cloud systems.

Disclosure of Customer Data:

eGT does not disclose or release customer data unless we are required to comply with law enforcement, federal or state regulations, or valid, binding order provided by government, law enforcement or regulatory bodies.

Protection of Customer Data:

To ensure the security of customer data provided to eGT, data is either kept in within the secure AWS partner portal used to provision services or within eGT owned and operated infrastructure. Any customer data kept on eGT infrastructure is only accessible by a limited number of authorized users and is encrypted both in transition and at rest.

eGT does not copy, disclose or retain any customer data or data derived from providing services for later use following completion of any contract services.

Role Based Access/Account Management:

eGT AWS cloud operations and support operate on the principals of least privilege and role-based access, only allowing authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. This best practice ensures that eGT personnel only have access to a limited set of customer data to perform tasks in support of the customer or to support eGT administrative activities.

The access roles provided below show the eGT personnel who may access the customer's environment and their role description. In these cases, access is only granted with permission from the customer and all actions performed by eGT within the customer's environment are tracked and audited. In addition, eGT personnel are required to establish strong passwords, or multi-factor authentication if available.

Role	Role Description
eGT Cloud Administrators	Has full administrative access the AWS partner portal and customer environment to provision and configuring cloud services for the customer.
eGT Cloud Engineers	Has limited access to the customer's components/environment needed to properly provide support, configure and deploy cloud services as required by the customer.
eGT DevOps	Limited access to the customer's development environment to assist the customer in developing and deploying applications.
eGT Project Manager	Does not have access to the customer's environment. Only has access to information provided by the customer for the purposes of facilitating AWS cloud projects.
Admin/Billing	Does not have access to the customer's environment. Only has access to information needed for customer billing or administrative functions needed to facilitate services.

Location of Data:

eGT ensures that AWS services provided to government customers only utilize availability zones where the data center is in the continental U.S. While cloud services are accessed remotely, eGT does not store any customer data on portal devices such as tablets or laptops.

Data Breach/Incident Notification

eGT reports any known breech or incident impacting the customer to the impacted customer by within 24 hours of discovery by telephone. eGT will then work with the customer if needed to remediate the breach/incident and provide lessons learned. eGT will investigate if the impact places the customer at risk for identity theft or fraud. eGT is aware that if a breach is a direct result of eGT's failure to meet its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the customer, eGT may be held financially responsible for remediation and notification activities.

Data Disposal:

Following the end of the contracted period of performance, eGT disposes of any customer engagement data by either erasing the data, erasure and physical destruction of the hard drives containing customer data or by formatting and overwriting customer data so it cannot be accessed.

6.2 Compliance with Applicable Data Privacy and Security Laws (8.5.2)

eGT follows all applicable federal and state privacy laws. eGT offers AWS services which are managed in alignment with regulations, standards, and best practices, including:

- FedRAMP
- SOCs 1, SOC 2, and SOC 3
- PCI DSS
- ISO 27001, 27017, 27018, and 9001
- Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6
- Federal Information Security Management Act (FISMA)
- US Health Insurance Portability and Accountability Act (HIPAA)
- FBI Criminal Justice Information Services (CJIS)
- NIST 800-171
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
- Family Educational Rights and Privacy Act (FERPA)
- Information Security Registered Assessors Program (IRAP) (Australia)
- IT-Grundschutz (Germany)

For information on all the security regulations and standards with which AWS complies, visit the AWS Compliance page (https://aws.amazon.com/compliance/).

eGT provided cloud services thorough AWS East/West and AWS GovCloud have been assessed and authorized under FedRAMP. The FedRAMP program requires AWS to comply with the following Federal, U.S. Code and State laws, including the E-Government Act of 2002 - FISMA of 2002, Title III.

Document Number/Code	Title
44 USC 31	Title 44 Public Printing and Documents; Chapter 31 Records Management by Federal Agencies
5 USC 552a	Title 5 Government Organization and Employees; Chapter 5 Administrative Procedure; Section 552a Records maintained on individuals (Privacy Act of 1974 as amended)
HSPD-12	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors [HSPD-12], August 27, 2004
HSPD-7	Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7], December 17, 2003
OMB Circular A-108	Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [, as amended]
OMB Circular A-123	Management's Responsibility for Internal Control Revised
OMB Circular A-130	Managing Information as a Strategic Resource
OMB M-01-05	Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
OMB M-03-22	OMB Guidance for Implementing the Privacy Provisions
OMB M-04-04	E-Authentication Guidance for Federal Agencies
OMB M-06-16	Protection of Sensitive Agency Information
OMB M-07-16	Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)
OMB M-10-23	Guidance for Agency Use of Third-Party Websites

Document Number/Code	Title
OMB M-99-18	Privacy Policies on Federal Web Sites
PL 99-474	Computer Fraud and Abuse Act, 18 USC 1030
PL 100-503	Consolidated Appropriations Act of 2005, Section 522
PL 104-191	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
PL 104-231	Electronic Freedom of Information Act As Amended in 2002 [PL 104-231, 5 USC 552], October 2, 1996
PL 107-56	USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)
PL 107-347	E-Government Act of 2002 - FISMA of 2002, Title III
PL 107-347 208	E-Government Act of 2002 - Sec. 208. Privacy provisions.
PL 107-347 V	E-Government Act of 2002 - The Confidential Information Protection and Statistical Efficiency Act (CIPSEA), Title V
PL 108-447	Consolidated Appropriations Act of 2005, Section 522
PL 113-187	44 U.S.C The Presidential and Federal Records Act Amendments of 2014 showing changes to NARA Statutes found below in Chapters 21, 22, 29, 31, 33, of Title 44 in PDF.
NARA	44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33 (see Public Law 113-187)
FTC	Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices
ECFR	Title 36, Code of Federal Regulations, Chapter XII, Subchapter B
NCSL	State Privacy Laws

As required by Utah state law, eGT is compliant with state codes protecting personal data.

eGT does not acquire personal data or non-public personal data during its work, and, prohibits the disclosure of non-public personal information in alignment of Utah Code §§ 13-37-201 to -203, *Notice of Intent to Sell Nonpublic Personal Information Act*.

In accordance with Utah Code Utah Code §§ 13-44102 – 301. *The Protection of Personal Information Act*, eGT maintains and implements processes, procedures and security controls to prevent the unlawful disclosure of customer information collected in the course of business. The procedures include:

- Implementing least privilege, limited access to information systems to only the personnel who require access order to support the customer.
- Encryption of customer data in transit and at rest.
- Implementation of network and vulnerability protection within eGT systems.

eGT also disposes of customer data, as required by Utah Code Utah Code §§ 13-44102 – 301, following the end of a contract or following the end of a customer engagement data by either erasing the data, erasure and physical destruction of the hard drives containing customer data or by formatting and overwriting customer data so it cannot be accessed.

While eGT does not acquire personal data or non-public personal data, in the case of a breach, as required by Utah Code Utah Code §§ 13-44102 – 301, eGT reports any known breach or incident impacting the customer to the impacted customer. eGT will then perform a prompt investigation to determine if the customer is at risk for identity theft or fraud.

6.3 Purchasing Entity's User Accounts or Data (8.5.3)

eGT's customers using AWS IaaS, retain ownership and control over their content within the AWS environment. They also retain responsibilities relating to the security of that content as part of the AWS "shared responsibility" model. While eGT along with AWS manages security of the cloud, security in the cloud is the responsibility of the customer, as customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks – no differently than they would for applications in an on-site data center.

eGT and AWS does not access or use customer content for any purpose other than as legally required and to provide the specific IaaS services selected by each customer, to that customer and its end users. Our managed cloud services team will have only limited and controlled access to customer data that will only be accessed in response to customer requests for system administration and maintenance activities such as backing up and restoring databases. eGT and AWS will never use customer content or derive information from it for other purposes, such as marketing or advertising.

7 Privacy and Security (8.6)

As an ACP offering AWS cloud services and an AFAQ ISO 27001 Information Security certified organization, eGT understands how important it is to protect customer data and ensure compliance with privacy and security regulations. eGT has put processes and policies in place to ensure the security of customer data. Maintaining the security of customer data and most importantly the trust of the customer is our key goal. eGT also offers AWS services which feature world class security, services and tools used to protect customer data. In addition, AWS underwent an extraordinarily thorough compliance exercise, ensuring that they meet the requirements of the FedRAMP, SOCs 1, SOC 2, and SOC 3, PCI DSS, and ISO 27001, 27017, 27018, and 9001.

7.1 Commitment to NIST Compliance (8.6.1)

eGT provides access to cloud computing solutions from AWS that have been certified, accredited and authorized to meet the requirements of NIST and federal security requirements under the FedRAMP. In addition, eGT personnel have a deep understanding of the NIST Risk Management Framework and worked the with FedRAMP PMO at the GSA to develop and launch the FedRAMP program.

Under the FedRAMP program AWS cloud services were assessed to meet the essential characteristics of cloud computing under NIST SP 800-145, The NIST Definition of Cloud Computing.

FedRAMP leverages the NIST Risk management framework under NIST SP 800-37 and, which requires:

1. Categorization
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System and monitor.
6. Monitor Security Controls

AWS East/West was categorized as a moderate impact system and AWS GovCloud was categorized as using guidance from FIPS 199, Standards for Security Categorization of Federal Information and Information Systems; NIST SP 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1; and NIST SP 800-60 Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1.

The controls selected for implementation are defined by the FedRAMP program and leverage the controls from NIST SP 800-53 rev. 4 Security and Privacy Controls for Information Systems and Organizations.

AWS has implemented the required controls and the implementation was tested and assessed by a FedRAMP certified third-party assessment organization/independent assessor and granted an authority to operate (ATO) by the FedRAMP Joint Authorization Board (JAB), which is composed of representative from the GSA, DHS, and DoD. The ATO for GovCloud was granted on June 21, 2016 at a high impact level and the ATO for AWS East/West was granted November 13, 2017 at a moderate impact level.

FedRAMP then performs continuous monitoring of the cloud system monthly to ensure the system maintains its risk posture.

For further verification, please see AWS whitepaper *Cybersecurity Framework (CSF) Aligning to the NIST CSF in the AWS Cloud*, which provides a third-party auditor letter validating attestation confirming AWS services' conformance to the NIST CSF risk management practices.

In addition, the FedRAMP program ensures that the AWS services provided by eGT meet the following NIST requirements and guidance:

Identification Number	Title
NIST SP 800-60	Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1
NIST SP 800-60	Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1
NIST SP 800-61	Computer Security Incident Handling Guide, Revision 2
NIST SP 800-63-2	Electronic Authentication Guideline: Computer Security, Revision 2
NIST SP 800-64	Security Considerations in the System Development Life Cycle, Revision 2
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
NIST SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations
NIST SP 800-122	NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NIST SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing
NIST SP 800-145	The NIST Definition of Cloud Computing
FTC	Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress
NARA 2010-05	Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)
FDIC	Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks

eGT has staff with expertise in the NIST Risk Management Framework and NIST 800-53 security controls to assist customers with understanding control inheritance and help them to implement hybrid and customer controls to secure their data.

As outlined in the AWS Control Implementation Summary, some controls may have a shared, customer-only or AWS only responsibility. Based on this model, control responsibility is as follows:

Shared Responsibility: You will provide security and configurations of your software components and AWS will provide security for its infrastructure.

Customer-Only Responsibility: You are fully responsible for guest operating systems, deployed applications, and select networking resources (for example, firewalls). More specifically, you are solely responsible for configuring and managing security "in" the cloud.

AWS-Only Responsibility: AWS manages the cloud infrastructure, including the network, data storage, system resources, data centers, physical security, reliability, and supporting hardware and software. Applications built on top of the AWS system inherit the features and configurable options that AWS provides. AWS is solely responsible for configuring and managing security "of" the cloud.

The portion of shared controls that the customer is responsibility for, and controls related to applications the customer implements on top of the AWS infrastructure, must be separately assessed and authorized in agreement with NIST 800-37 and customer-specific security authorization policies and procedures.

7.2 Government, Standard Organization Security Certifications (8.6.2)

eGT holds the following industry certifications

- AWS certified eGT as an ACP and “Public Sector Partner”
- Microsoft Cloud Solutions Provider
- CMMIDEV/4 (Appraisal# 26869)
- AFAQ ISO 27001 Information Security certified organization
- AFAQ ISO 20000-1 IT Service Management
- AFAQ ISO 9001 Quality
- Project Management Professional
- Certified Information Systems Security Professional (CISSP)

AWS Compliance and Security Certifications (For information on all the security regulations and standards with which AWS complies, visit the AWS Compliance page

- FedRAMP
- SOCs 1, SOC 2, and SOC 3
- PCI DSS
- ISO 27001, 27017, 27018, and 9001
- DoD SRG Impact Levels 2, 4, 5, and 6
- FISMA
- HIPAA
- FBI CJIS
- NIST 800-171
- ITAR
- FIPS 140-2
- FERPA
- IRAP (Australia)
- IT-Grundschutz (Germany)

7.3 Security Practices to Secure Data and Applications (8.6.3)

eGT, a significant provider of cybersecurity management and enforcement to the government, possesses end-to-end security capabilities that protects systems and data from inception to retirement.

eGT leverages an optimal, and continuously improving, blend of monitoring tools that proactively identify suspicious activities from the network ingress points, to the operating system and at the application stack. To do this, eGT leverages AWS built in monitoring capabilities that monitors networks and cloud resources by leveraging port scanning, network usage, application

usage and failed authenticate and authorization attempts. AWS employs triggers to provide automated alerts and notifications to enable rapid response to emerging security threats.

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

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

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

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

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

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

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

Port Scanning. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via the contacts available on our website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and can only be opened by a customer. Srict management of security groups by customers, can further mitigate the threat of port scans. If customers configure the security

group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. In these cases, customers must use appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. For example, a web server must clearly have port 80 (HTTP) open to the world, and the administrator of this server is responsible for the security of the HTTP server software, such as Apache. You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

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

7.4 Data Confidentiality Standards and Practices (8.6.4)

eGT partners with AWS to provide self-service capabilities to allowing customers to fully provision and manage their own environments. We do not directly access any of the cloud assets except to provide customer service and only for that purpose. We do not access customer data, and customers assume the responsibility of determine storage methodologies, data management and data protection policies. eGT may assist the clients in helping determine the best policies; however, would not require direct access to the data.

7.4.1 Prevention of Exposure and Managing Access

Our AWS offering provides numerous security layers to help customers secure and protect their data. Resources may be protected at the application, storage, cloud resource and network layers among other. Clients may precisely control access to data to ensure that only authorized users can configure cloud storage resources and who can see the data within those resources. AWS provides countless resources to enable monitoring and auditing of data access across each of the data storage cloud services. See section 7.6 for additional auditing capabilities. These logging and auditing capabilities range from S3 storage object access, file system access, database access through application data access. AWS provides the ability to restrict access to specific hardware through numerous means including private VPN access, IP restrictions and via two-factor authentication.

eGT provides value add consulting services to help clients define and implement their data access policies for cloud and on-premise solutions.

7.5 List of Third-Party Attestations, Reports, Security Credentials, and Certifications (8.6.5)

Compliance certifications and attestations are assessed by a certified third-party, independent auditor respective to each program and result in a certification, audit report, or attestation of compliance.

AWS is FedRAMP compliant and have been granted authorizations since addressing all FedRAMP security controls (based on NIST SP800-53) by the third-party assessor 3PAO and maintains continuous monitoring requirements.

AWS GovCloud (US), has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for **high impact level**. The services in scope of the AWS GovCloud (US) JAB P-ATO boundary at **high baseline security categorization** can be found within AWS Services in Scope by Compliance Program.

AWS US East-West, has been granted a JAB P-ATO and multiple A-ATO for **moderate impact level**. The services in scope of the AWS US East-West JAB P-ATO boundary at **Moderate baseline security categorization** can be found within AWS Services in Scope by Compliance Program.

The following table details additional certifications and attestations:

Certifications/Attestations:	Laws/Regulations/Privacy:	Alignments/Frameworks:
C5 [Germany]	Argentina Data Privacy	CIS
Cyber Essentials Plus [UK]	CISPE	CJIS
DoD SRG	EU Model Clauses	CSA
FedRAMP	FERPA	ENS High [Spain]
FIPS	GDPR	EU-US Privacy Shield
IRAP [Australia]	GLBA	FFIEC
ISO 9001	HIPAA	FISC
ISO 27001	HITECH	FISMA
ISO 27017	IRS 1075	G-Cloud [UK]
ISO 27018	ITAR	GxP (FDA CFR 21 Part 11)
K-ISMS [Korea]	My Number Act [Japan]	ICREA
MTCS [Singapore]	U.K. DPA - 1988	IT Grundschutz [Germany]
PCI DSS Level 1	VPAT/Section 508	MITA 3.0
SEC Rule 17-a-4(f)	EU Data Protection Directive	MPAA
SOC 1	Privacy Act [Australia]	NIST
SOC 2	Privacy Act [New Zealand]	PHR
SOC 3	PDPA - 2010 [Malaysia]	Uptime Institute Tiers
	PDPA - 2012 [Singapore]	UK Cloud Security Principles
	PIPEDA [Canada]	
	Spanish DPA Authorization	

Additional information is available here - https://aws.amazon.com/compliance/programs/.

7.6 Logging Process (8.6.6)

eGT recognizes the logging and monitoring of Application Program Interface (API) calls as key components in security and operational best practices, as well as requirements for industry and regulatory compliance. AWS provides multiple features and capabilities to monitor, manage and analyze log files:

AWS CloudTrail is a web service that records API calls to supported AWS services within AWS accounts and delivers a log file to the Amazon S3 bucket. AWS CloudTrail alleviates common challenges experienced in an on-premise environment and in addition to making it easier to demonstrate compliance with policies or regulatory standards, the service makes it easier to enhance security and operational processes. It logs systems and applications and Amazon S3 and AWS Lambda data events.

- Amazon S3 Data Events - API activity on Amazon S3 Objects.
- AWS Lambda Data Events - execution activity of Lambda functions.

Information fields include API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation).

The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

By default, CloudTrail log files are encrypted using S3 Server Side Encryption (SSE) and placed into your S3 bucket. You can control access to log files by applying IAM or S3 bucket policies. You can add an additional layer of security by enabling S3 Multi Factor Authentication (MFA) Delete on your S3 bucket."

Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by customer applications and services, and any log files that applications generate.

Customers can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. It logs systems and applications and AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by customer applications and services, and any log files that applications generate. Customers can send their existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time. This helps customers better understand and operate their systems and applications, and they can store their logs using highly durable, low-cost storage for later access.

Security certifications will be maintained by utilizing the features described above to monitor, manage and analyze logs and reports in conjunction with the AWS Auditing Security Checklist (https://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf). While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an onsite datacenter. As part of the AWS Auditing Security Checklist, eGT would

take the approach to assign the AWS account and resource owner, as well as the AWS services and resources being utilized to the designated customer. In addition, eGT's approach is to validate that audit logging is being performed on the guest OS and critical applications installed on AWS instances and that implementation is in alignment with policies and procedures, especially as it relates to the storage, protection, and analysis of the logs which include the following:

Logging Assessment Trails and Monitoring. Review logging and monitoring policies and procedures for adequacy, retention, defined thresholds and secure maintenance, specifically for detecting unauthorized activity for AWS services.

- Review logging and monitoring policies and procedures and ensure the inclusion of AWS services, including Amazon EC2 instances for security related events.
- Verify that logging mechanisms are configured to send logs to a centralized server.
- Ensure that for Amazon EC2 instances, the proper type and format of logs are retained in a similar manner as with physical systems.
- For customers using AWS CloudWatch, review the process and record of the use of network monitoring.
- Ensure analytics of events are utilized to improve defensive measures and policies.
- Review AWS IAM Credential report for unauthorized users, AWS Config and resource tagging for unauthorized devices.
- Confirm aggregation and correlation of event data from multiple sources using AWS services.

Intrusion Detection and Response. Review host-based IDS on Amazon EC2 instances in a similar manner as with physical systems.

- Review AWS provided evidence on where information on intrusion detection processes can be reviewed.

7.7 Restricting Visibility of Cloud Hosted Data and Documents (8.6.7)

eGT can restrict visibility of cloud hosted data and documents to specific users or groups. The AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Using IAM, customers can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. IAM allows customers to:

- Manage IAM users and their access – Customers can create users in IAM, assign them individual security credentials (e.g., access keys, passwords, and multi-factor authentication devices) or request temporary security credentials to provide users access to AWS services and resources. Customers can manage permissions in order to control which operations a user can perform.
- Manage IAM roles and their permissions – Customers can create roles in IAM and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. Customers can also define which entity can assume the role.

- Manage federated users and their permissions – Customers can enable identity federation to allow existing identities (e.g., users) in the enterprise to access the AWS Management Console, to call AWS APIs, and to access resources, without the need to create an IAM user for each identity.

7.8 Security Incident Notification Process (8.6.8)

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

In addition, The Amazon CloudWatch monitoring service is used to collect and track metrics, collect and monitor log files, and as it relates, set custom metrics for alarms and notifications. Third-party compatibility to monitor and analyze are also available so that existing tools can also be utilized.

7.9 Physical and Virtual Security Controls (8.6.9)

The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI QSA and resulted to be in compliance with all requirements of PCI DSS version 3.2 published in April 2016. More information on AWS's multi-tenant architecture is found in the AWS Risk and Compliance whitepaper: https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.

AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS Cloud while isolating your Amazon EC2 compute instances at the hardware level. Additional information on Dedicated Instances can be found at http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated-instance.html.

AWS isolation and deployment options are illustrated below in **Figure 3.**

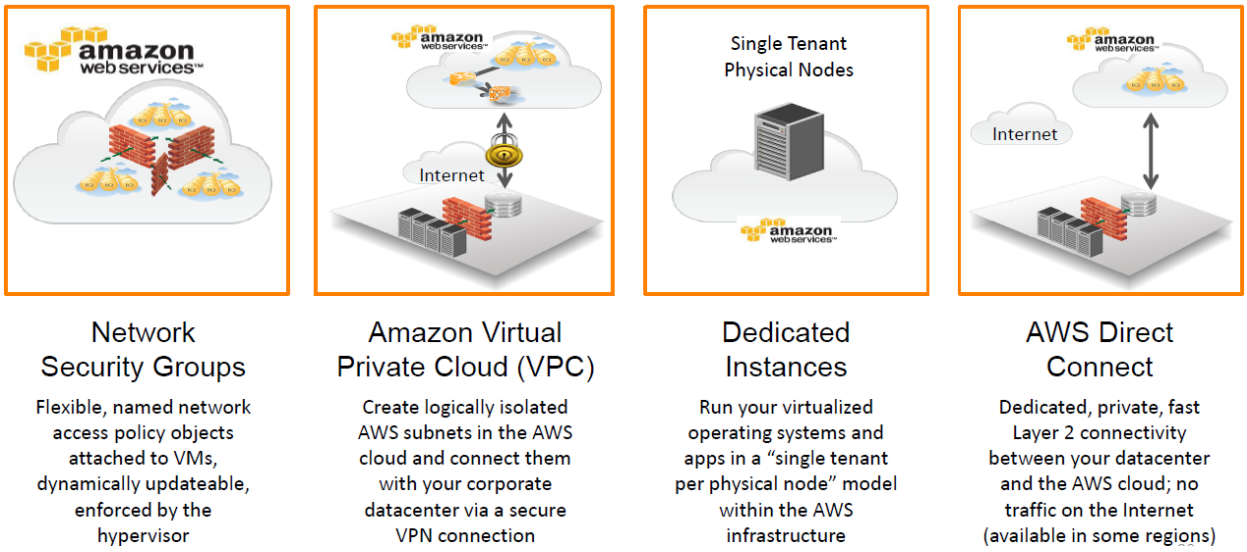


Figure 3 | AWS Isolation and Deployment Options

7.10 Security Technical Reference Architectures (8.6.10)

Cloud computing architectures is broad and continuously evolving. As each use case and requirements are unique, eGT will evaluate how best to implement the desired services to the cloud. Once so, important principles and design procedures will be instilled. Additional guidance is detailed in the following AWS whitepapers:

Architecting for the Cloud: AWS Best Practices (February 2016) contains prescriptive guidance for architects designing solutions with AWS services.
https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf

Managing Your AWS Infrastructure at Scale Feb 2015 contains information on tools and techniques for managing your AWS environment at any scale.
https://d0.awsstatic.com/whitepapers/managing-your-aws-infrastructure-at-scale.pdf

Additional whitepapers are located at: https://aws.amazon.com/whitepapers/

7.11 Security Procedures Regarding Employees (8.6.11)

eGT has an internal dedicated Human Resources Department as well as annual mandatory training via its eGT University portal for its staff. As part, all employees are required to complete Code of Business Conduct and Ethics training which is a key part of eGTs ethical framework. All staff supporting Federal or State customers are required to comply with the Compliance Basics of Federal Contracting Compliance Policy.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and customers are responsible for securing the workloads they deploy in AWS. AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts pre-employment criminal background checks, as permitted by law, for employees commensurate with their position and level of access. The AWS SOC reports provide additional details regarding the controls in place for background verification.

7.12 Security Measures and Standards to Secure Data Confidentiality at Rest and in Transit (8.6.12)

AWS customers retain control and ownership of their data, and all data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. AWS offers the ability to add an additional layer of security to data at rest in the cloud by providing scalable and efficient encryption features. This includes:

- Data encryption capabilities in AWS storage and database services, such as Amazon EBS, Amazon S3, Amazon Glacier, Oracle RDS, SQL Server RDS, and Amazon Redshift.
- Flexible key management options, including AWS Key Management Service, that allow customers to choose whether to have AWS manage the encryption keys or keep complete control over their keys.
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing customers to satisfy compliance requirements.
- Support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit.
- Application Programming Interfaces (APIs) for customers to integrate encryption and data protection with any of the services developed or deployed in an AWS environment.

The AWS Security Best Practices whitepaper (https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf) provides greater detail on how to protect data in transit and at rest in the AWS Cloud. Other security resources are also available on the AWS Cloud Security Resources page, https://aws.amazon.com/security/security-resources/.

7.13 Policies and Procedures to Notify State and Cardholders of Data Breaches and Mitigation of Breaches (8.6.13)

AWS has implemented a formal, documented incident response policy and program. AWS Customers retain the responsibility to monitor their own environment for privacy breaches. Please refer to 4.1 Data Breach for additional information.

In addition to the internal communication mechanisms detailed in 4.1 Data Breach, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" (http://status.aws.amazon.com/) is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

8 Migration and Redeployment Plan (8.7)

8.1 End of Life Activities (8.7.1)

eGT offers complete cloud migration and implementation services from start to finish. We leverage our DevOps Factory framework and methodology to streamline and automate cloud migration projects. As opposed to simply doing a lift-and-shift of a customer workload from on-premise to cloud environment, we automate the end-to-end deployment process and transform the workload thereby optimizing performance and operations in the cloud. We will work with Purchasing Entities, in establishing a comprehensive project plan that covers activities prior, during and post migration and implementation of workloads in the cloud platform. At the conclusion of project, we will coordinate with Purchasing Entities to initiate a set of end of life activities that includes, transfer of cloud accounts and access privileges, transfer of any data assets, and safe deprovisioning of any environments prior to termination of the contract. We consider each customer project to be unique and will work with users to identify and address all known and unknown activities.

In accordance with the shared responsibility model, Purchasing Entities can either directly manage the creation and deletion of their compute and storage resources or contract through eGT to provide such managed cloud services. Customer will have direct capability to decommission any service at any time either through a well-defined AWS provided API or from a system console. At all times, including during the closing down of a service, controls are in place limit access to systems and data and access to systems or data is restricted and monitored. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, and FedRAMP audits.

8.2 Return of Data (8.7.2)

Migration of data to either another Cloud vendor or to the customer’s site is completely under the control of the customer. AWS provides many mechanisms that can be used in migrating data, again completely under the control of the customer. Further, AWS does not store data in a proprietary format, which makes the data portable. The following are a few of the more common methods available for data migration.

Unstructured files can be copied using many standard copy command, the AWS APIs and/or the AWS Console. For example, moving data from AWS S3 Object Storage can be performed simply by the customer issuing a simple AWS CLI copy command.

The customer can use AWS’ S3 Object Storage to migrate data. S3 provides a means, with extensive access controls and authentication methods, to allow access to data through an URL. The customer can move data to S3, such as an Oracle database export, and download the file to either another Cloud provider or an on-premise system. The data can also be encrypted for greater security.

AWS provides Snowball, a petabyte-scale data transport solution that uses devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud. Snowball is an excellent method for large datasets and files where using standard communications lines would not be feasible due to the amount of time needed for the migration.

AWS provides Data Migration Service, which allows the replication and migration of data from AWS to on premise databases. The service supports most common database management systems including Oracle, SQL Server, MySQL, and Postgres.

The customer can use any off-the-self or user written migration application that can be run on an AWS EC2 instance. For example, a Customer can use standard Oracle migration tools, such as Data Pump, to move data from AWS to on premise.

Customers have numerous options for redundancy during data migration. First, data can be migrated while maintaining the data at AWS. Only after the migration is complete and the results verified does the customer need to delete the source data. Second, data at AWS can be backed up in numerous ways, such as to Glacier, a low-cost storage option. However, since all the migration techniques discussed above are non-disruption, backing up the data is not normally required. Third, many AWS storage services provide direct support to maintain data across redundant systems including across different AWS datacenters and regions. For example, most AWS database services allow for multi-region support, which is enabled through a simple configuration setting.

9 Service or Data Recovery (8.8)

eGT recognizes the importance in quickly and efficiently recovering data and services in the case of an incident. This infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. The systems are designed to tolerate system or hardware failures with minimal customer impact. Data center Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group.

eGT's high availability cloud architecture for FEMA Disaster Management Support Environment (DMSE) ensured the seamless and elastic growth of the environment by over 400% with no impact to services and performance.

Availability.

Our AWS offering is built in clusters in various global regions. All data centers are online and serving customers, so there are no "cold" data centers. In case of failure, automated processes are in place to move customer data traffic away from the affected area. Also by deploying core applications in an N+1 configuration, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites if a data failure should occur.

eGT and AWS will provide you with the flexibility to place instances and store data within multiple geographic regions, as well as across multiple availability zones within each region. Each of these availability zones are designed as an independent failure zone, meaning they are physically separated within a typical metropolitan region. They are also located in lower risk flood plains based on the flood zone categorizations of the locations' Region. To further reduce single points of failure, these data centers have discrete uninterruptable power supply (UPS) and onsite backup generation facilities, as well as they are each fed via different grids from independent utilities. Availability zones are also all redundantly connected to multiple tier-1 transit providers.

You will be able to architect your usage to take advantage of multiple regions and availability zones. By distributing applications across multiple availability zones, the data will remain more resilient in the face of most failure modes, including natural disasters or system failures.

Fault-Tolerant Design.

Our infrastructure has a high level of availability and provides you with the capability to deploy a resilient IT architecture. The systems are designed to tolerate system or hardware failures with minimal customer impact. This fault-tolerant design allows for a variety of technologies to take your data to the next level with serverless computing, such as cost and space efficiency and accountability during high traffic times.

While you can architect your usage to take advantage of multiple regions and availability zones, you should be aware of location-dependent privacy and compliance requirements. Data is not replicated between regions unless the customer does so, which allows customers with these types of data placement and privacy requirements to establish compliant environments. It should be noted that all communications between regions is across public Internet infrastructure, so appropriate encryption methods should be used to protect sensitive data.

Currently, there are five available regions in the continental US: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West). The GovCloud (US) Region is isolated so to allow US government agencies and customers the ability to move workloads into the cloud and adhering to certain regulatory and

compliance requirements. US government agencies and their contractors using the GovCloud framework are compliant with U.S. ITAR regulations as well as the FedRAMP requirements. This GovCloud (US) has been authorized with an Agency Authorization to Operate (ATO) from the US Department of HHS utilizing a FedRAMP accredited Third-Party Assessment Organization (3PAO).

The GovCloud (US) Region provides the same fault-tolerant design as other regions and has two Availability Zones. The GovCloud (US) region also is a mandatory AWS Virtual Private Cloud (VPC) service by default. This creates an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private (RFC 1918) addresses. More information about GovCloud is available here: http://aws.amazon.com/govcloud-us/

9.1 Contingency Plan/Policy (8.8.1)

Businesses are using the AWS Cloud to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS Cloud supports many popular disaster recovery (DR) architectures from “pilot light” environments that may be suitable for small customer workload data center failures to “hot standby” environments that enable rapid failover at scale. With data centers in 13 regions around the world, AWS provides a set of cloud-based DR services that enable rapid recovery of your IT infrastructure and data. Most organizations choose to implement High Availability (HA) instead of Disaster Recovery to guard them against any downtime of services. In case of HA, we ensure there exists a fallback mechanism for our services. The service that runs in HA is handled by hosts running in different availability zones but in the same geographical region.

Situation	eGT Response
a. Extended downtime.	This infrastructure is modeled to actively avoid extended downtime through the use of regions and Availability Zones. If downtime is to occur, eGT will work adamantly with AWS to get the systems back up and running. A Service Credit may be applicable.
b. Suffers an unrecoverable loss of data.	AWS offers managed file and database storage with robust backup and restore capabilities that is distributed across multiple availability zones mitigating data loss risks
c. Offeror experiences a system failure.	By storing data and data backups in multiple regions, the user has a more resilient infrastructure for their information. If a system failure were to occur in a region or Availability Zone, it would be transferred to another region until the other system is back online.
d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.	We strive for an RTO of 4 hours. In most cases, the data will be available in another region or Availability Zone, so systems are frequently able to fail and recover with no interruption to the user.
e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).	We have an RPO of 24 hours. This means that for recovery, our data can’t be older than 24 hours. Our RTO, meaning the time it takes to complete the restoration from the time the DR is declared, varies from six hours to 24 hours based on the customer SLA. The details will also be available in the agreed SLA and Contingency Plan.

9.2 Backup and Restore Methodologies (8.8.2)

In most traditional environments, data is backed up to tape and sent off-site regularly, which can lead to long recovery times and increased costs. We can offer storage solutions designed to provide the reliability, durability, and scalability needed for various sizes of organizations and projects, without the need for any on premise infrastructure. Using Amazon S3 is ideal for backup data, as it is designed to provide 99.99% durability of objects over a given year. Transferring data to and from Amazon S3 is typically done via the network, and it is therefore accessible from any location. If you choose to, you can automatically back up on-premises data to Amazon S3 with AWS Storage Gateway. Using Amazon Glacier also provides efficient, cost-effective, and scalable solutions for long term backups.

Backup and Restore Service	eGT Methodology
a. Method of data backups	All cloud service providers (CSPs), eGT has partnered with, such as AWS provide comprehensive data backup and retention capabilities in all of their service offerings. For instance, the AWS RDS supports both manual and automated backups and in the case of the latter it creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. You can set the backup retention period when you create a DB instance. If you do not set the backup retention period, Amazon RDS uses a default period retention period of one day. You can modify the backup retention period; valid values are 0 (for no backup retention) to a maximum of 35 days. Manual snapshot limits (50 per region) do not apply to automated backups.
b. Method of server image backups	Our cloud orchestration approach incorporates automated cron jobs that backup all databases and file systems to Amazon Elastic Block Store (EBS) volumes. These backups are performed hourly, daily, and weekly per requirements and are appropriately named and tagged for quick and rapid retrieval. Different storage classes, Standard, One Zone, and Glacier, allow the client to optimize cost and purpose. Backups can be stored in a Glacier server, since it does not need frequent accessibility. This allows the necessary or frequently used data to exist within Standard storage and maximize the utilization of space. Our high availability architecture with multiple node clusters provides sufficient redundancy reducing risk of failures and non-availability. Our management of digital platform cloud through tools like Cloudamatic®, enables us to issue a single command for restoring backups of database and file systems assuring Mean Time To Recover (MTTR) is less than 15 minutes and Mean Time Between Failures is no shorter than 30 days. Using Zendesk, we also publish self-help resources and points and methods of contact for communicating service outages and technical and security issues. This is further broken down by Tier 1, 2, 3, and 4 and established response time for each tier. The specific SLAs are further elaborated on in the Quality Assurance Plan.
c. Digital location of backup storage (secondary storage, tape, etc.)	Currently, there are 18 regions, 54 Availability Zones, and one Local Region throughout the world. These include US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia).
d. Alternate data center strategies for primary data centers within the continental U.S.	A multi-site solution runs in AWS and on your existing on-site infrastructure in an active-active configuration. Utilizing Route 53 will assist in this by allowing you to define your four hosted zones. During a disaster situation, you can send all traffic to AWS servers, which can scale to handle your full production load. Although rare, failures that affect the availability of instances in the same location can occur. Since your data can be moved to different hosted zones, you will face minimal downtime. We recommend that customers replicate data in different Availability Zones to ensure swift recovery in case of disaster.

10 Data Protection (8.9)

eGT will use standard encryption technologies—such as automated AWS encryption solutions, manual client-side options, protecting network traffic between clients and servers, and protecting network traffic between servers—to secure data while in transit or at rest. The team is willing to sign a Business Associate Agreement or any other agreement to protect data with the Purchasing Entity and will only use data as defined in the Master Agreement, participating addendum, or related SLA.

10.1 Standard Encryption Technologies and Options (8.9.1)

Securing Data in Transit

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

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

The AWS Security Best Practices whitepaper (https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf) provides greater detail on how to protect data in transit and at rest in the AWS Cloud.

Additionally, eGT's SiteMonitor tool informs system owners whether or not their security protocols are meeting government compliance standards. SiteMonitor secures data in transit by scanning TLS conformance of applications and informing system owners about what actions to take to better secure their data to meet government protocols.

Securing Data at Rest

There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions (such as AWS Key Management Service [KMS], which facilitates creating and controlling encryption keys used to encrypt data, and uses FIPS 140-2 validated hardware security modules to protect the security of keys) to manual, client-side options (such as AWS CloudHSM, a cloud-based hardware security module [HSM] which makes it easy to generate and use a user's own encryption keys on the AWS Cloud).

Choosing the right solutions depends on which AWS Cloud services are being used and customer requirements for key management. Information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon S3 Developer Guide (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html).

Additionally, FIPS 140-2 validated encryption is available in GovCloud. FedRAMP requires FIPS 140-2 validated or NSA compliant crypto.

More information is available in the Encrypting Data at Rest whitepaper (https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_ with_Encryption.pdf), which provides an overview of the options for encrypting data at rest in AWS Cloud services. It

describes these options in terms of where encryption keys are stored and how access to those keys is controlled. Both server-side and client-side encryption methods are discussed with examples of how each can be accomplished in various AWS Cloud services.

10.2 Business Associate Agreement (8.9.2)

eGT is willing to sign a relevant and applicable Business Associate Agreement (BAA) or any other agreement that may be necessary to protect data with a Purchasing Entity. eGT has a standard BAA we present to customers for signature. It takes into account the unique services AWS provides and accommodates the AWS Shared Responsibility Model.

eGT will ensure its compliance with the European Union's (EU) General Data Protection Regulation (GDPR). Any personal identifiable information (PII) or behavioral data collected over the internet from an EU country will adhere to the requirements in the GDPR, and eGT will ensure the data is protected under the GDPR's rules.

10.3 Data Usage (8.9.3)

eGT will only use data for purposes defined in the Master Agreement, participating addendum, or related SLA. eGT will not use the government data or government related data for any other purpose including but not limited to data mining. eGT will not resell nor otherwise redistribute information gained from its access to the data received as a result of the RFP.

eGT does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. eGT does not sell or share customer data for purposes such as marketing or advertising in any way.

11 Service Level Agreements (8.10)

eGT will leverage AWS to provide Purchasing Entity's with cloud hosting services and will maintain and comply with AWS's SLA for services. In addition, our SLA would also meet service level requirements related to disaster recovery (DR), continuity of operations (COOP), help desk support, security (such as FedRAMP, FISMA), governance and other such similar requirements. We will partner with Purchasing Entity to collaboratively develop and refine the service level requirements for such support services. We comply with Amazon's EC2 SLA available through AWS website.

11.1 Negotiability of SLA (8.10.1)

eGT is committed in providing excellent cloud services to Purchasing Entities. Our proposed Infrastructure as-a Service solution namely AWS has millions of active Customers worldwide. The AWS SLA establishes high standards for reliability, availability and uptime and therefore is not negotiable. eGT is willing to discuss with Purchasing Entities to review and evaluate any new SLA requirements with respect to managed cloud services and incorporate them if appropriate and acceptable. AWS offers the same portfolio of self-service and highly automated web services to its customers on a one-to-many basis. Because of this, AWS is unable to commit to keep the Services or SLAs the same for certain customers but improve or change them for others. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 100 services that range from compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid, and enterprise applications.

11.2 Sample SLA (8.10.2)

In the following table we capture a sample of SLAs for our Managed Cloud Services and our approach for the various service level requirements that we offer to the Purchasing Entity.

SLA	Our Approach
Meet Availability Service Levels.	Depending on the support plan, technical support is available either during local business hours all the way up to 24x7 Real-time access and visibility to log issues via email and customer portal.
Meet Service Level Time to Respond (Acknowledge) to Requests Service Levels	All support requests will be acknowledged in a timely manner with most requests receiving a response within four hours or less if reported within core availability hours.
Meet Mean-Time-To-Resolve Service Levels (F.3)	eGT will make every effort to resolve support tickets in a timely manner, however the time to resolve support tickets would vary based on the type of support issue. Mean-Time-To-Resolve is based on the severity of the issue and any dependency on third party vendors. We propose the following MTTR service levels. Access/Password Reset – 24 hours for approved requests received Monday through Thursday in a given week. AWS instances – stand up within 48 hours for approved requests Monday through Wednesday in a given week. eGT will work with Purchasing Entity's PMO to further define and refine the service levels to meet the organizational requirements.

SLA	Our Approach
Meet Middleware Management Service Level Requirements	eGT will work with Purchasing Entity in scheduling patch updates and ensure stakeholders are notified sufficiently in advance for any outages. Patch updates will be sufficiently tested and validated prior to implementation.

The following table captures a few sample SLAs offered by AWS.

AWS SLA	Service Commitment	Service Credits	SLA Exclusions
Amazon Cloud Front SLA	AWS will use commercially reasonable efforts to make Amazon CloudFront available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the "Service Commitment"). In the event Amazon CloudFront does not meet the Service Commitment, Purchasing Entity will be eligible to receive a Service Credit.	Service Credits are calculated as a percentage of the total charges paid by Purchasing Entity for Amazon CloudFront for the billing cycle in which the error occurred in accordance with the schedule below. • 10% Service Credit for a monthly uptime % >= 99% but <99.9% • 25% Service Credit for a monthly uptime is <99%	The Service Commitment does not apply to any unavailability, suspension or termination of Amazon CloudFront, or any other Amazon CloudFront performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon CloudFront; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use Amazon CloudFront in accordance with the AWS Agreement; (vi) that result from exceeding usage limits stated in the Amazon CloudFront documentation; or (vii) that result from use of an origin server other than Amazon S3 (collectively, the "Amazon CloudFront SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of the Error Rate, then we may issue a Service Credit considering such factors at our discretion.
Amazon EC2 SLA	AWS will use commercially reasonable efforts to make the Included Products and Services each available with a Monthly Uptime Percentage (defined below) of at least 99.99%, in each case during any monthly billing cycle (the "Service Commitment"). In the event any of the Included Products and Services do not meet the Service	Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for either Amazon EC2 or Amazon EBS (whichever was Unavailable, or both if both were Unavailable) in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below, • 10% Service Credit for a monthly uptime % <	The Service Commitment does not apply to any unavailability, suspension or termination of Amazon EC2 or Amazon EBS, or any other Amazon EC2 or Amazon EBS performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon EC2 or Amazon EBS; (iii) that result from any actions or inactions of you or any third party, including failure to acknowledge a recovery volume; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from failures of individual instances or

AWS SLA	Service Commitment	Service Credits	SLA Exclusions
	Commitment, Purchasing Entity will be eligible to receive a Service Credit	99.99% but >= 99.0% • 30% Service Credit for a monthly uptime is <99%	volumes not attributable to Region Unavailability; (vi) that result from any maintenance as provided for pursuant to the AWS Agreement; or (vii) arising from our suspension and termination of your right to use Amazon EC2 or Amazon EBS in accordance with the AWS Agreement (collectively, the "Amazon EC2 SLA Exclusions"). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.
Amazon S3 SLA	AWS will use commercially reasonable efforts to make Amazon S3 available with the applicable Monthly Uptime Percentage (as defined below) during any monthly billing cycle (the "Service Commitment"). In the event Amazon S3 does not meet the Service Commitment, you will be eligible to receive a Service Credit	Service Credits are calculated as a percentage of the total charges paid by you for Amazon S3 for the billing cycle in which the error occurred in accordance with the schedule below. For all requests not otherwise specified below: • 10% Service Credit for a monthly uptime % >= 99.0% but < 99.9% • 30% Service Credit for a monthly uptime is <99.0% For requests to Amazon S3 Standard – Infrequent Access (Standard-IA) and Amazon S3 One Zone – Infrequent Access (OneZone-IA): • 10% Service Credit for a monthly uptime % >= 98.0% but < 99.0% • 25% Service Credit for a monthly uptime is <98.0%	The Service Commitment does not apply to any unavailability, suspension or termination of Amazon S3, or any other Amazon S3 performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon S3; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (v) arising from our suspension and termination of your right to use Amazon S3 in accordance with the AWS Agreement (collectively, the "Amazon S3 SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of the Error Rate, then we may issue a Service Credit considering such factors at our discretion.
Amazon Route 53 SLA	AWS will use commercially reasonable efforts to make Amazon Route 53 100% Available (defined below). In the event Amazon Route 53 does not meet the foregoing commitment, Purchasing Entity	Service Credits are calculated based on one day of Service Credit, which is equal to your average daily Amazon Route 53 query charges for the monthly billing cycle preceding the monthly billing cycle in which the period that Amazon Route 53 was not 100% Available occurred, and are available	The Service Commitment does not apply to any unavailability, suspension or termination of Amazon Route 53, or any other Amazon Route 53 performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon Route 53; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your

AWS SLA	Service Commitment	Service Credits	SLA Exclusions
	will be eligible to receive a Service Credit	as follows: • 1-day Service Credit for a 5-30minutes duration Amazon Route 53 was not 100% available • 7-days Service Credit for a 31minutes -4hours duration Amazon Route 53 was not 100% available • 30-days Service Credit for more than 4-hours duration Amazon Route 53 was not 100% available	equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use Amazon Route 53 in accordance with the AWS Agreement; (vi) that result from you exceeding usage limits stated in the Amazon Route 53 documentation; or (vii) that, with respect to public DNS only, result during a period that you were not using all four virtual name servers (for example, ns123.awsdns.com, ns123.awsdns.net, ns123.awsdns.co.uk and ns123.awsdns.org) assigned to your "hosted zone" (collectively, the "Amazon Route 53 SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of 100% Available, then we may issue a Service Credit considering such factors at our discretion.
Amazon Relational Database Service (Amazon RDS) SLA	AWS will use commercially reasonable efforts to make Multi-AZ instances available with a Monthly Uptime Percentage (defined below) of at least 99.95% during any monthly billing cycle (the "Service Commitment"). In the event Amazon RDS does not meet the Monthly Uptime Percentage commitment, Purchasing Entity will be eligible to receive a Service Credit	Service Credits are calculated as a percentage of the charges paid by you for the Multi-AZ instances that did not meet the Monthly Uptime Percentage commitment in a billing cycle in accordance with the schedule below. • 10% Service Credit for a monthly uptime % < 99.95% but >= 99.0% • 25% Service Credit for a monthly uptime is <99.0%	The Service Commitment does not apply to any unavailability, suspension or termination of Amazon RDS, or any other Amazon RDS performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon RDS; (iii) that result from any voluntary actions or inactions from you or any third party (e.g., rebooting a database instance, scaling compute capacity, not scaling storage when the storage is full, misconfiguring security groups, VPC configurations or credential settings, disabling encryption keys or making the encryption keys inaccessible, etc.); (iv) that result from instances belonging to the Micro DB instance class or other instance classes which have similar CPU and memory resource limitations; (v) that result from you not following the basic operational guidelines described in the Amazon RDS User Guide (e.g., overloading a database instance to the point it is inoperable, creating excessively large number of tables that significantly increase the recovery time

AWS SLA	Service Commitment	Service Credits	SLA Exclusions
			etc.); (vi) caused by underlying database engine software that lead to repeated database crashes or an inoperable database instance; (vii) that result in long recovery time due to insufficient IO capacity for your database workload; (viii) that result from your equipment, software or other technology and/or third-party equipment, software or other technology (other than third party equipment within our direct control); or (ix) that result from any maintenance as provided for pursuant to the AWS Agreement; or (x) arising from our suspension and termination of your right to use Amazon RDS in accordance with the AWS Agreement (collectively, the "Amazon RDS SLA Exclusions"). If availability is impacted by factors other than those explicitly used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.
AWS Shield Advanced SLA	For Amazon CloudFront and Amazon Route 53 resources designated by you for protection by AWS Shield Advanced, AWS will use commercially reasonable efforts to prevent those resources from failing to meet any service commitments specified in the Amazon CloudFront SLA or Route 53 SLA as a result of any denial-of-service attack covered by	For each 24-hour period (Coordinated Universal Time) in which Amazon CloudFront or Amazon Route 53 experienced an availability interruption that contributed to AWS Shield Advanced not meeting the Service Commitment you are entitled to a “Service Credit” in an amount equal to the average daily charges for AWS Shield Advanced for the monthly billing cycle in which the Service Commitment failure occurred. We will apply any Service Credits only against future AWS Shield Advanced payments otherwise due from you. At our discretion, we may	Not Applicable

AWS SLA	Service Commitment	Service Credits	SLA Exclusions
	AWS Shield Advanced (the "Service Commitment"). In the event AWS Shield Advanced does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below. For Amazon CloudFront and Amazon Route 53 resources designated by you for protection by AWS Shield Advanced, a denial-of-service attack covered by AWS Shield Advanced will not constitute an Amazon CloudFront SLA Exclusion or Amazon Route 53 SLA Exclusion (as defined in the Amazon CloudFront Service Level Agreement and the Amazon Route 53 Service Level Agreement, respectively) with respect to a failure to meet any service commitments specified in the Amazon CloudFront Service Level Agreement or Route 53 Service Level Agreement.	issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service Commitment failure occurred. Service Credits will not entitle you to any refund or other payment from AWS. Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement (including the Amazon CloudFront SLA or Amazon Route 53 SLA), your sole and exclusive remedy for any unavailability of the AWS resources designated by you for protection by AWS Shield Advanced is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.	

12 Data Disposal Procedures and Policies (8.11)

eGT is committed to protecting our customer’s data assets in the cloud and promptly disposing it on conclusion of the contract. Leveraging AWS, we ensure customers retain control and ownership of their data, and it is the customer's responsibility to manage their data, including the ability to delete their data at any point. On receiving an official request from a customer to dispose and delete their data, eGT initiates the following activities:

- Identify the data volumes that should be deleted and secure confirmation of disposal from customer.
- eGT initiates process to permanently delete the data from the file system or database by completely deprovisioning the specific cloud resources.
- When a storage device within AWS cloud has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.
- On completion, eGT provides a confirmation notice, confirming the permanent destruction of the data.

13 Performance Measures and Reporting (8.12)

Service commitments to performance are described in detail in **Section 11.2**. eGT is dedicated to optimizing the reliability of AWS and delivering clear and measurable support on demand. Below we elaborate our ability to guarantee reliability and uptime and methods of seeking technical support.

13.1 Guarantee of Reliability and Uptime over 99.5% (8.12.1)

In 2014, Nucleus Research surveyed 198 AWS customers that reported moving existing workloads from on-premises to AWS and found that they were able to reduce unplanned downtime by 32% (see Availability and Reliability in the Cloud: AWS).

eGT in partnership with AWS can offer 99.9% or higher reliability and uptime for most of the services. AWS replicates critical system components across multiple Availability Zones to ensure high availability both under normal circumstances and during disasters such as fires, tornadoes, or floods. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Each AWS Availability Zone runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single Availability Zone. The data centers' electrical power systems are designed to be fully redundant and maintainable without impact to operations. Common points of failure, such as generators, UPS units, and air conditioning, are not shared across Availability Zones.

AWS plans for failure by maintaining contingency plans and regularly rehearsing our responses. AWS regularly performs preventative maintenance on our generators and UPS units to ensure that equipment is ready when needed. AWS also maintains a series of incident response plans covering both common and uncommon events and updates them regularly to incorporate lessons learned and prepare for emerging threats.

While AWS goes to great lengths to provide availability of the cloud, customers share responsibility for ensuring availability within the cloud. These customers and others like them have succeeded because they designed for failure and have adopted best practices for high availability, such as taking advantage of multiple Availability Zones and configuring Auto Scaling groups to replace unhealthy instances. The **Building Fault-Tolerant Applications on AWS** (https://aws.amazon.com/whitepapers/designing-fault-tolerant-applications/) whitepaper is a great introduction to achieving high availability in the cloud. In addition, the **AWS Well-Architected Framework** (http://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf) codifies the experiences of thousands of customers, helping customers assess and improve their cloud-based architectures and mitigate disruptions.

In addition, the **AWS Architecture Center** (https://aws.amazon.com/architecture/) is designed to provide customers with the necessary guidance and application architecture best practices to build highly scalable and reliable applications in the AWS Cloud. These resources will help you understand the AWS Cloud, its services and features, and will provide architectural guidance for design and implementation of systems that run on the AWS infrastructure.

13.2 Standard Uptime Service and Related SLA Criteria (8.12.2)

AWS far exceeds the Uptime Institute Tiering certification. Tiering aspects do not take into consideration the nature of the services of the cloud environment, and although the uptime institution tiering can be a great guide, it ultimately does not accurately map to a Cloud Service Provider (CSP) organization. AWS does not have a Certified Uptime Tiering level; however, we operate a data center environment using N+1 architecture. AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.95%, and Amazon S3 with an SLA of 99.9%. Our generator backup capabilities are detailed in our SOC Reports (as is our discussion regarding business continuity planning and N+1 architecture).

13.3 Support (8.12.3)

Purchasing Entities will have the ability to seek support by creating trouble tickets through an on-line portable hosted and managed by AWS. Upon creation of this ticket, purchasing entities can use email mechanisms or the portal to follow-up and receive updates on their support request. AWS additionally supports a 24x7x365 technical support hotline that can be used to escalate high priority issues. AWS offers multiple support plans including Developer, Business and Enterprise. Depending on the selected plan, we offer email and phone access with turnaround time in less than one hour for high severity cases to less than 24 hours for general guidance. More details of the support plans can be found here - https://aws.amazon.com/premiumsupport/

13.4 Failure to Meet Incident Response Time and Incident Fix Time (8.12.4)

Please refer to the information provided in response to **Section 11 – Service Level Agreements**.

13.5 Procedures and Schedules for Planned Downtime (8.12.5)

AWS does not require systems to be brought offline to perform regular maintenance and system patching, and AWS's own maintenance and system patching generally do not impact customers. There may be occasions when AWS might schedule a customer instance for a reboot for necessary maintenance, such as to apply updates that require a reboot. No action is required on the customer's part; we recommend that customers wait for the reboot to occur within its scheduled window. These scheduled events are not frequent and if a customer instance will be affected by a scheduled event, they will receive an email prior to the scheduled event with details about the event, as well as a start and end date. Customers can also view scheduled events for their instance(s) by using the Amazon EC2 Console, API, or CLI. AWS will communicate with customers, either via email, or through the AWS Service Health Dashboard if service use is likely to be adversely affected.

13.6 Failure to Meet Disaster Recovery Metrics (8.12.6)

Please refer to the information provided in response to **Section 11 – Service Level Agreements**.

13.7 Sample Performance Reports (8.12.7)

AWS customers can leverage AWS Cloud monitoring tools such as Amazon CloudWatch, AWS Trusted Advisor, AWS Health Checks, and third-party monitoring tools to extract metrics and system analytics.

Performance reports are available over the Web through the **AWS Service Health Dashboard** (http://status.aws.amazon.com/), which provides current and historical data across regions for each service offered. The status can be monitored in real-time or subscribed to as an RSS feed by service. AWS performance reports can be configured to provide both real-time and historical statistics for a specific range of date and time period. **Figure 4** is an example of a performance report that denotes the geographical distribution of requests received by a Cloud Front internet gateway.

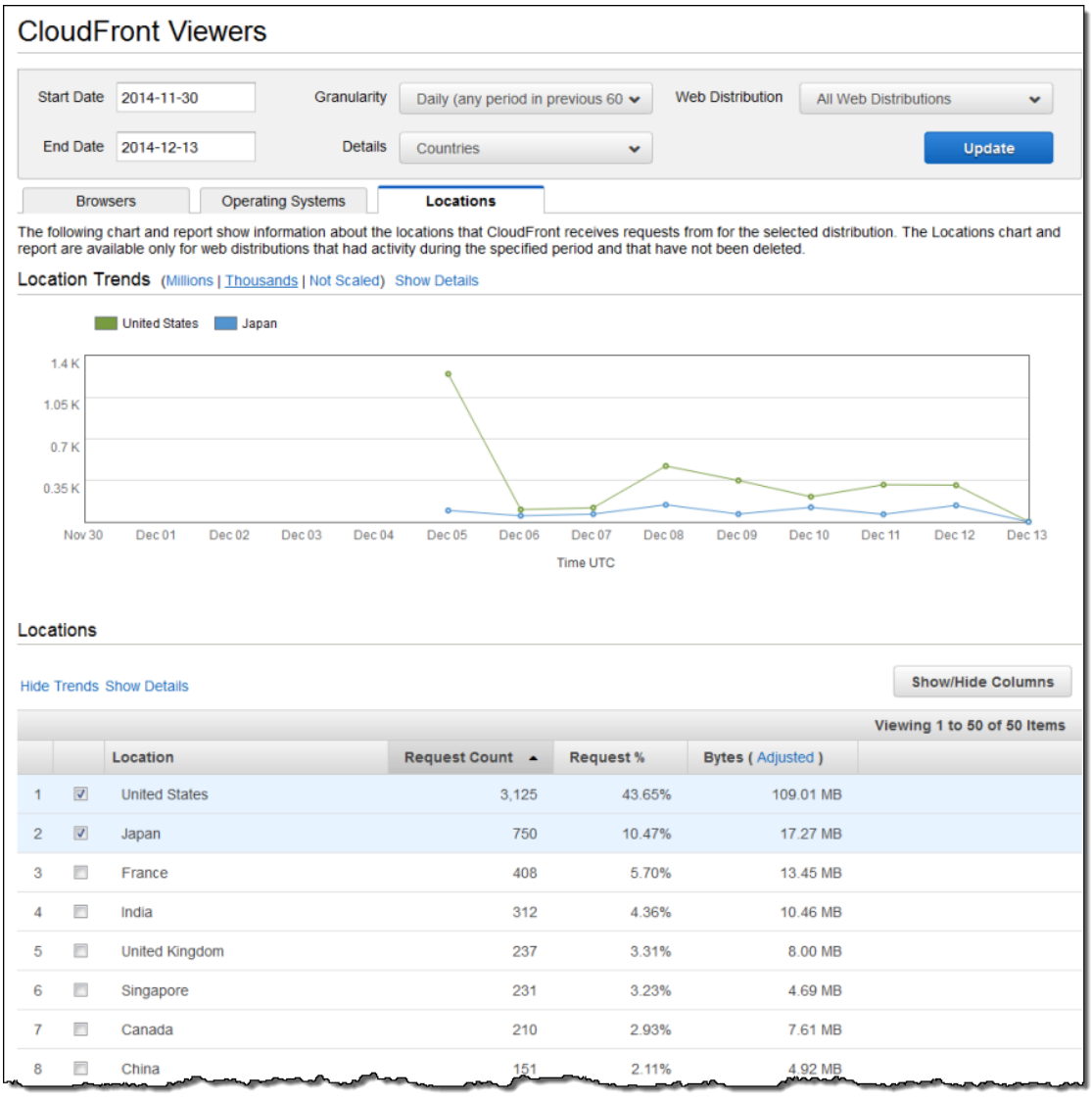


Figure 4 | Sample Performance Report

13.8 Historical, Statistical and Usage Reports (8.12.8)

eGT's proposed IaaS solution, AWS, has multiple services that provide historical, statistical and usage reports available through the AWS Management Console that can also be exported to PDF and other file formats and can be printed locally. AWS CloudWatch is one such service that can monitor user configured resources and applications in real-time. Users can use CloudWatch to collect and track metrics for their resources and applications and report them through a variety of graphs, visualizations and list them in a tabular manner.

CloudWatch not only allows for real-time reports but also historical reports, dashboards, statistics, usage and alerts (e.g., notification of a service exceeding a pre-set cost budget). Reports can be viewed on the CloudWatch console or printed for offline use. **Figure 5** depicts the features and capabilities supported AWS CloudWatch.

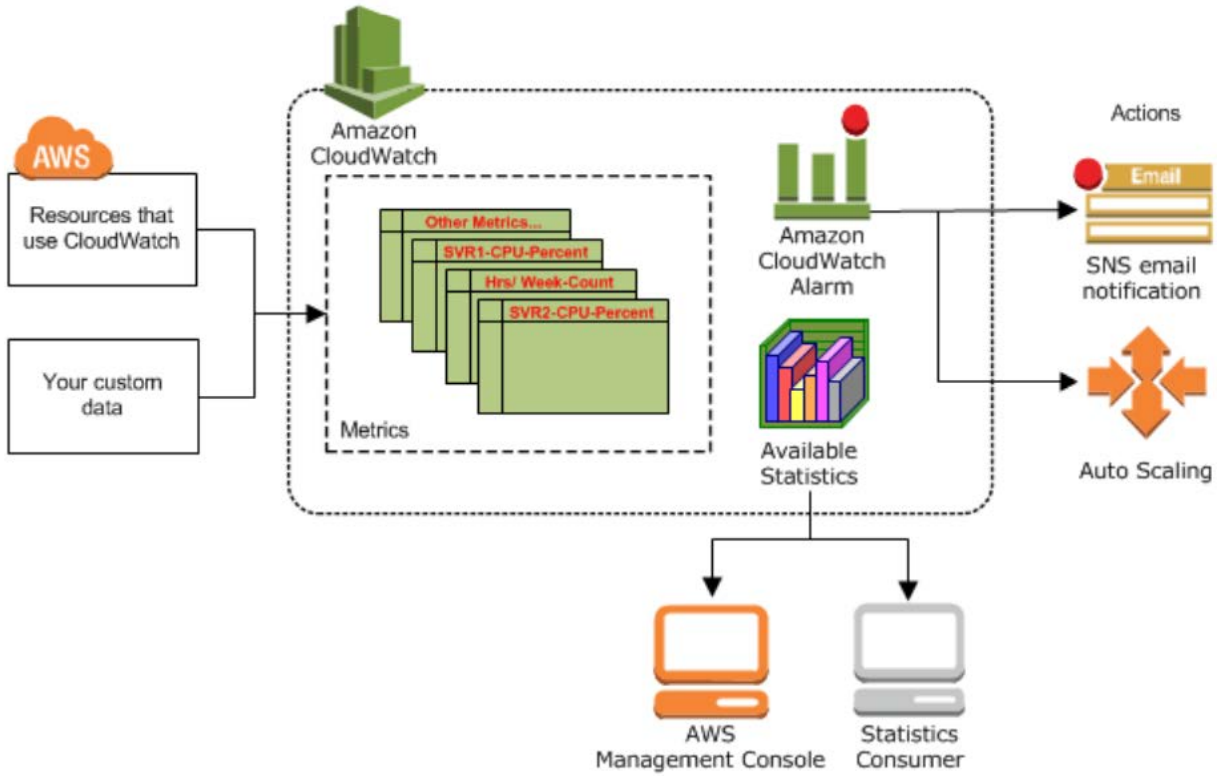


Figure 5 | Features and Capabilities Supported AWS CloudWatch

CloudWatch logs can also be downloaded and used by the customer with other third-party log management or reporting tools. For example, a Customer can download CloudWatch logs and do complex analysis using SAS or ServiceNow thereby consolidating alerting and incident reporting.

13.9 On-Demand Deployment (8.12.9)

AWS provides on-demand capabilities of all services 24x7x365. AWS offers you a pay-as-you-go approach for pricing for 70+ cloud services. With AWS you pay only for the individual services you need, for as long as you use them, and without requiring long-term contracts or complex licensing. AWS pricing is similar to how you pay for utilities like water or electricity.

You only pay for the services you consume, and once you stop using them, there are no additional costs or termination fees. Services can be started/created and stopped/destroyed manually by the client or through numerous automation techniques.

AWS also provides other pricing options that can significantly reduce overall costs to the Customer. For example, Reserved Instances provide you with a significant discount compared to On-Demand Instance pricing whereby the Customer “purchases” a certain capacity. Reserved Instances are not physical instances, but rather a billing discount applied to the use of On-Demand Instances in your account.

13.10 Scale-Up and Scale-Down (8.12.10)

Auto Scaling allows customers to automatically scale their Amazon EC2 capacity up or down according to conditions that they define. Auto Scaling is well suited for applications that experience hourly, daily, or weekly variability in usage. Customers can automatically scale their Amazon EC2 fleet or maintain their Amazon EC2 fleet at a set size.

Auto Scaling enables customers to closely follow the demand curve for their applications, reducing the need to provision Amazon EC2 capacity in advance. For example, customers can set a condition to add new Amazon EC2 instances in increments of three instances to the Auto Scaling Group when the average CPU utilization of the Amazon EC2 fleet goes above 70%; and similarly, customers can set a condition to remove Amazon EC2 instances in the same increments when CPU utilization falls below 10%.

Often, customers may want more time to allow their fleet to stabilize before Auto Scaling adds or removes more Amazon EC2 instances. Customers can configure a cool down period for their Auto Scaling Group, which tells Auto Scaling to wait for some time after taking an action before it evaluates the conditions again. Auto Scaling enables customers to run their Amazon EC2 fleet at optimal utilization.

Amazon Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables customers to achieve even greater fault tolerance in their applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored. Customers can enable Elastic Load Balancing within a single Availability Zone or across multiple zones for even more consistent application performance.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track

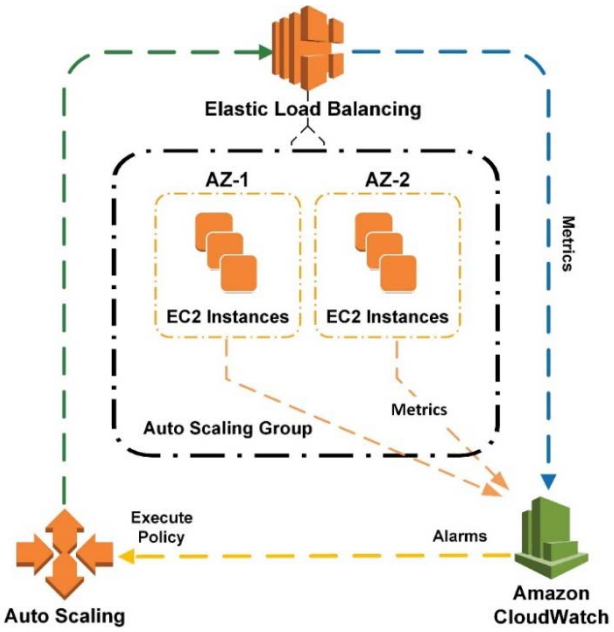


Figure 6 | Auto Scaling with Elastic Load Balancing and Amazon CloudWatch alarms

metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS database instances, as well as custom metrics generated by applications and services and any log files your applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react and keep application running smoothly.

Amazon CloudWatch's metrics and alarms can work together with Auto Scaling and ELB to dynamically deploy new instances on-demand.

14 Cloud Security Alliance (8.13)

eGT and AWS share the mission to promote the use of best practices for providing security assurances within cloud computing. As such, AWS participates in the Cloud Security Alliance (CSA) organization to achieve its mission.

14.1 Level of Disclosure with CSA Star Registry

CSA STAR Level 1: CSA STAR Self-Assessment (a & b)

AWS has completed the CSA STAR Self-Assessment and published the results to the AWS website. Please refer to the CSA Consensus Assessments Initiative Questionnaire document titled "**CSA_Consensus_Assessments_Initiative_Questionaire.pdf**".

CSA STAR Level 2: CSA STAR Attestation and Certification (c)

Per the CSA definitions, AWS aligns with the CSA STAR Attestation and Certification via the determinations in our third-party audits for SOC and ISO:

CSA STAR Level 2 Attestation is based on SOC2, which can be requested with AWS Artifact - The SOC 2 report audit attests that AWS has been validated by a third-party auditor to confirm that AWS' control objectives are appropriately designed and operating effectively. Please refer to the documents "**AWS-SOC-2-Oct17-Mar18.pdf**" and "**AWS-SOC2-Excel-Spreadsheet-Oct17-Mar18.xlsx**".

CSA STAR Level 3: Continuous Monitoring (d)

As noted on the CSA website (https://cloudsecurityalliance.org/star/continuous/), CSA is still defining the Level 3 Continuous Monitoring requirements. Although, for this reason, AWS cannot determine alignment, AWS does provide customers with the tools they need to meet continuous monitoring requirements. Customers can leverage the AWS Security by Design (SbD) program by providing control responsibilities outlines, the automation of security baselines, the configuration of security and the customer audit of controls for AWS customer infrastructure, operating systems, services and applications running in AWS. This standardized, automated, prescriptive and repeatable design can be deployed for common use cases, security standards and audit requirements across multiple industries and workloads. For more information visit the Security by Design page, https://aws.amazon.com/compliance/security-by-design/.

CSA STAR Level 2 Certification is based on ISO 27001:2005. Please see document **"iso_27001_global_certification .pdf**".

15 Service Provisioning (8.14)

eGT's proposed IaaS solution, AWS is a highly "elastic" platform providing the ability to provision computing resources in order of minutes and scale them up and down easily, with minimal friction. The elastic nature of AWS helps customers to avoid purchasing resources and services up front for projects and instead switch to a "just-in-time" model and provision just the required amount of resources when needed and deprovision them when no longer required, paying only for the actual duration of usage. AWS provides multiple interfaces for service provisioning and management that includes the AWS Management Console, APIs and variety of automation tools that can optimize and reduce the time taken to provision resources at scale. AWS also offers elastic load balancing and auto scaling capabilities that can be suitably configured to autonomously scale up and scale down resources based on demand. These unique features of AWS help optimize and reduce the investment cost for Purchasing Entities.

15.1 Emergency or Rush Services Implementation (8.14.1)

Purchasing Entities requiring a service request to be fulfilled immediately will have the option to utilize the AWS Management Console or appropriate interfaces to perform and implement the required changes independently at any time, 24x7x365. They can also use the AWS Management Console to initiate a support request and elevate the priority for resolution. eGT and AWS will promptly address such support requests adhering to the established SLA s as described in **Section 11 – Service Level Agreements**

15.2 Standard Lead-Time (8.14.2)

Our AWS offering does not require a lead time as AWS has both user interfaces and scriptable programming interfaces to provision services at any time and is typically fulfilled in the order of minutes. Purchasing Entities will have the required permissions to AWS Management Console or the programmable interfaces, to provision AWS resources independently. If Purchasing Entities will require eGT's assistance and support to provision services on behalf of their users, they can create a technical support ticket which will be fulfilled as per the SLAs described in **Section 11 – Service Level Agreements**.

16 Back Up and Disaster Plan (8.15)

eGT recognizes the importance and significance of the data it works with. The team is committed to establishing and maintaining a back-up plan and a disaster plan to act as a safety net in the event of an incident. On top of providing reliable back up and disaster plans, eGT can also provide guidance and consultation to help you formulate and execute the best plans for you and your data.

16.1 Applying Legal Retention Periods (8.15.1)

You, as the customer, will have control the entire life-cycle of their content on AWS. They also manage their content in accordance with their own specific needs, including content classification, access control, retention and deletion. If you are required to follow a legal, you can easily designate the records retention time frame to retain regulatory archives in the original form for the required duration. You can also place legal holds to retain data indefinitely until the hold is removed. This is done through Object Lifecycle Management. To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle.
A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

- **Transition actions** define when objects transition to another storage class. For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them. There are costs associated with the lifecycle transition requests.
- **Expiration actions**: Define when objects expire. S3 deletes expired objects on your behalf. The lifecycle expiration costs depend on when you choose to expire objects.

16.2 Known Inherent Disaster Recovery Risks and Potential Mitigation Strategies (8.15.2)

The infrastructure used by eGT and AWS has a high level of availability and you are provided the features needed to deploy a resilient IT architecture. The systems are designed to tolerate system or hardware failures with minimal customer impact. The available recovery architectures range from “pilot light” environments that are ready to scale up at a moment’s notice to “hot standby” environments, which enable rapid failover. This differs from a traditional hosting or local cloud because the we do not require the user to switch environments manually. Most AWS failover strategies require minimal effort for disaster recovery. Frequently it can be done automatically and within minutes.

All data centers are online and serving customers, so no data center is “cold.” If a failure incident were to occur, the automated processes move your data traffic away from the affected area. When you distribute applications across multiple AWS Availability Zones, your data can remain resilient in the face of most failure modes, including natural disasters or system failures. Highly resilient systems can be built in the cloud by employing multiple instances in multiple AWS Availability Zones and using data replication to achieve extremely high recovery time and recovery point objectives. You, as the customer, are responsible for managing and testing the backup and recovery of your information system that is built on the AWS infrastructure. Utilizing the available infrastructure enables faster disaster recovery of your critical IT systems without incurring the infrastructure expense of a second physical site.

16.3 Data Center Infrastructure (8.15.3)

The cloud infrastructure is built around regions and Availability Zones. A region is defined as a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each housed in separate facilities and built with redundant power, networking, and connectivity. There are five US regions: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California) and AWS GovCloud (US-West). Using these Availability Zones offers customers the ability to operate more highly available production applications and databases, as well as make them more fault tolerant and scalable than would be possible with a single data center.

These Availability Zones and regions create an environment with better failover for the user. The user can do real-time replication of data or databases within an Availability Zone, between an Availability Zone, and even between regions. The user has the ability to engineer their data and their replication so that they have multiple active or active for scale systems. Also, in case of an Availability Zone experiencing an incident, the data will be secure in a different Availability Zone, lessening the chance of data loss. We are also able to provide international support if requested through 13 other regions: Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia).

Figure 7 depicts the current Regions and Availability Zones, along with the four new regions that AWS has announced plans for.

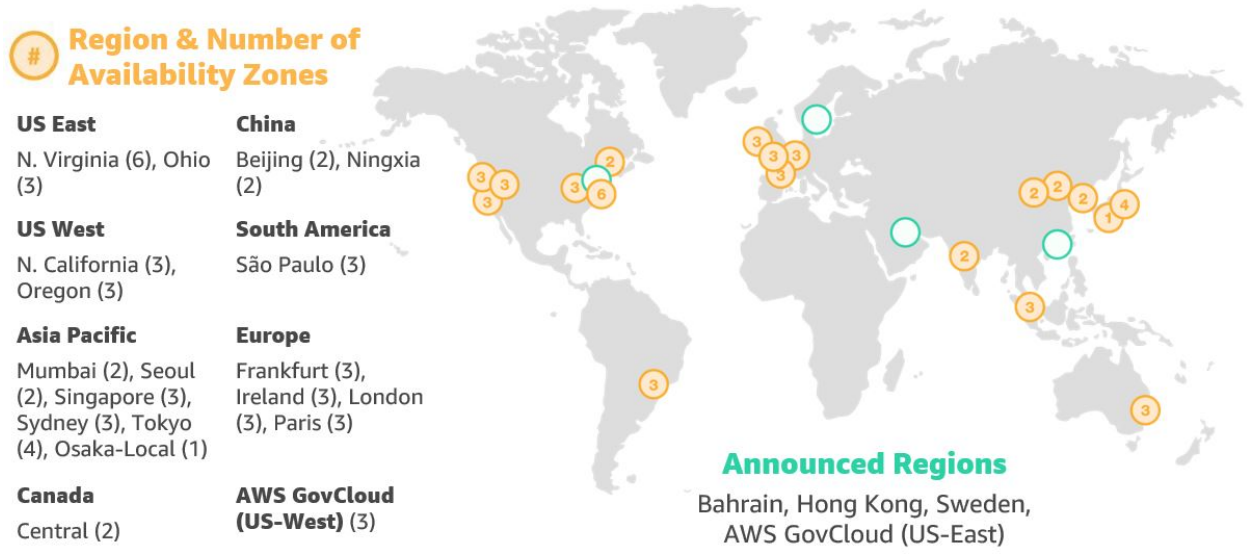


Figure 7 | Global Map of AWS Regions and Availability Zones

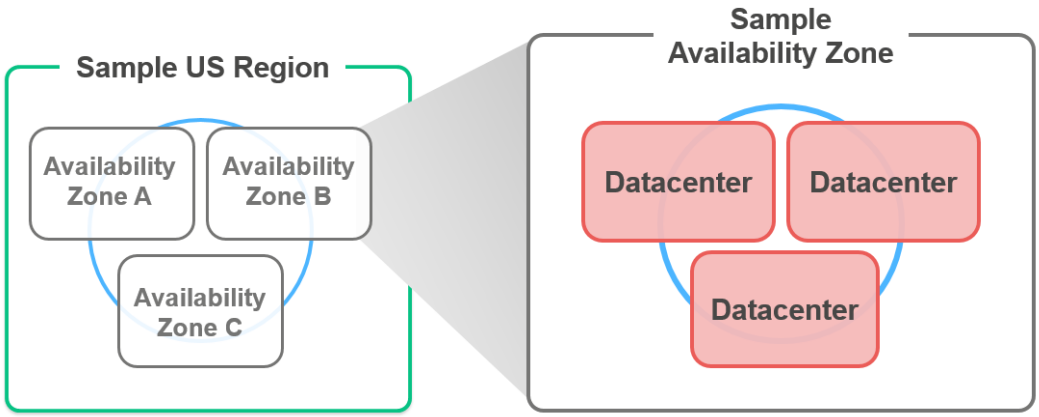


Figure 8 | Regions and Availability Zones

17 Hosting and Provisioning (8.16)

eGT will facilitate and support the planning of the hosting and provisioning requirements along with the implementation by utilizing the AWS Management Console which is a single destination for managing all AWS. The AWS Management Console can be accessed from http://aws.amazon.com/console/.

17.1 Documented Cloud Hosting Provisioning Process (8.16.1)

The AWS Management Console is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) (http://aws.amazon.com/ec2/) instances to Amazon DynamoDB (http://aws.amazon.com/dynamodb/) tables. Customers can use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS IAM (http://aws.amazon.com/iam/) users. The AWS Management Console supports all AWS Regions (http://aws.amazon.com/about-aws/globalinfrastructure/) and lets customers provision resources across multiple regions.

17.1.1 Defined/Standard Cloud Provisioning Stack

AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS API-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits, and Command Line Tools: http://aws.amazon.com/tools/.

17.2 Tool Sets (8.16.2)

The AWS Developer Tools (https://aws.amazon.com/products/developer-tools/) help you securely store and version control your application's source code and automatically build, test, and deploy your application to AWS or your on-premises environment.

The AWS Command Line Interface (CLI) (http://aws.amazon.com/cli/) is a unified tool used to manage AWS Cloud services. With just one tool to download and configure, customers can control multiple AWS resources from the command line and automate them through scripts. The AWS CLI introduces a new set of simple file commands (http://aws.amazon.com/cli/?nc1=h_l2_dm#file_commands_anchor) for efficient file transfers to and from Amazon S3 (http://aws.amazon.com/s3/).

17.2.1 Deploying New Servers (1)

AWS CodeBuild (https://aws.amazon.com/codebuild/) is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. With AWS CodeBuild, customers don’t need to provision, manage, and scale their own build servers. AWS CodeBuild scales continuously and processes multiple builds concurrently, so builds are not left waiting in a queue. Customers can get started quickly by using prepackaged build environments, or they can create custom build environments that use their own build tools. With AWS CodeBuild, customers are charged by the minute for the compute resources they use.

AWS CodeDeploy (https://aws.amazon.com/codebuild/) is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for customers to rapidly release new features, helps them avoid downtime during application deployment, and handles the complexity of updating their applications. Customers can use AWS CodeDeploy to automate software deployments, eliminating the need for error-prone manual operations. The service also scales with infrastructure, so customers can easily deploy to one instance or thousands.

AWS CloudFormation (https://aws.amazon.com/cloudformation/) gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Customers can use AWS CloudFormation's sample templates or create their own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run their application.

AWS Marketplace (https://aws.amazon.com/marketplace) is an online store that helps customers find, buy, and immediately start using the software and services they need to build products and run their businesses. AWS Marketplace features many software categories including databases, application servers, testing tools, monitoring tools, content management, and business intelligence. Visitors to AWS Marketplace can use 1-Click deployment to quickly launch pre-configured software and pay only for what they use, by the hour or month. AWS handles billing and payments, and software charges appear on customers' AWS bill.

AWS Service Catalog (https://aws.amazon.com/servicecatalog/) allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, helps them achieve consistent governance, and helps them meet their compliance requirements, all while enabling users to quickly deploy only the approved IT services they need.

17.2.2 Creating and Storing Server Images (2)

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments. OpsWorks has three offerings, **AWS Opsworks for Chef Automate, AWS OpsWorks for Puppet Enterprise**, and **AWS OpsWorks Stacks**.

AWS Systems Manager (https://aws.amazon.com/ec2/systems-manager/) allows customers to centralize operational data from multiple AWS services and automate tasks across AWS resources. Customers can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. With AWS Systems Manager, customers can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. AWS Systems Manager provides a central place to view and manage AWS resources, so customers can have complete visibility and control over their operations.

17.2.3 Securing Additional Storage Space (3)

AWS Trusted Advisor (https://aws.amazon.com/premiumsupport/trustedadvisor/) is an online resource to help customers reduce cost, increase performance, and improve security by optimizing their AWS environment. AWS Trusted Advisor provides real-time guidance to help customers provision their resources following AWS best practices and onto storage media such as EBA, S3 and Glacier. The S3 media features the ability to automatically scale to ensure minimal administration as storage requirements change.

17.2.4 Monitoring Tools (4)

Amazon CloudWatch (https://aws.amazon.com/cloudwatch/) is a monitoring service for AWS Cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon Relational Database Service (Amazon RDS) DB instances, as well as custom metrics generated by the customer's applications and services and any log files their applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health and then use those insights to react and keep their application running smoothly.

AWS provides a broad set of services that help IT administrators, systems administrators, and developers more easily manage and monitor their resources. Using these fully managed services, customers can automatically provision, configure, and manage their AWS or on-premises resources at scale. Customers can also monitor infrastructure logs and metrics using real-time dashboards and alarms. AWS also helps customers monitor, track, and enforce compliance and security.

AWS Config (https://aws.amazon.com/config/) is a fully managed service that provides customers with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config Rules enables customers to create rules that automatically check the configuration of AWS resources recorded by AWS Config. With AWS Config, customers can discover existing and deleted AWS resources, determine their overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

AWS CloudTrail (https://aws.amazon.com/cloudtrail/) is a web service that records AWS API calls for a customer's account and delivers log files to them. The recorded information 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 AWS Cloud service. With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS Cloud services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

18 Trial and Testing Periods (Pre- and Post-Purchase) (8.17)

In this section, we describe the testing and training periods and services we offer as part of our overall service offering.

18.1 Testing and Training Periods (8.17.1)

eGT in partnership with AWS, offer both no-cost and class room training services. The period and duration of training can vary from one day to one week, dependent on the specific training program and session. Details about AWS training programs are available here - https://aws.amazon.com/training/. These training services are available during the pre and post purchase phases.

eGT provides Incubation as-a Service to customers as part of its Research & Development (R&D) arm, called eGT Labs. Through this program we offer AWS-based hosting environments for customers for short-time periods that can be used by them for testing and evaluation during pre and post purchase phases.

18.2 Test and/or Proof of Concept Environment (8.17.2)

eGT, as part of its eGT Labs program, maintains a lab environment hosted on AWS for testing and prototyping purposes. This environment can be made available to customers, if and when required, to test, evaluate, prove and verify compliance to the mandatory minimum requirements.

18.3 No-Cost Training Support (8.17.3)

eGT's proposed IaaS provider, AWS offers free on-line training and is designed to let customers learn at their own pace. It provides access to on-demand self-paced digital courses like *AWS Cloud Practitioner Essentials*, *Big Data Technical Fundamentals*, *Security Fundamentals*, and *Job Roles in the Cloud*. Customers can explore the catalog of digital training courses on this website - https://aws.amazon.com/training/course-descriptions/

19 Integration and Customization (8.18)

eGT's proposed IaaS and PaaS solution AWS, is 100% API driven using REST services. This enables standards-based integration with other applications, systems and cloud providers. AWS provides the scaffolding and mechanisms to build interoperable applications. In the following sections, we further describe how AWS supports and can be used in a manner to facilitate standards-based integration with complementary applications

19.1 Standards-Based Integration Capabilities (8.18.1)

All AWS services can be utilized and managed through well-defined REST based APIs. This allows users to utilize either the AWS Management Console, available out of the box or any popular cloud security, management and automation tools such as Telos Xacta 360, Cloud Checkr, Chef, Puppet, and Ansible. These complementary tools enable the secure and efficient usage of cloud platforms including AWS, in a vendor agnostic manner enabling customers to adopt and utilize multiple IaaS and PaaS platforms. Amazon API Gateway is an AWS service that enables developers to create, publish, maintain, monitor, and secure APIs at any scale. Customers can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud. API Gateway can be considered a backplane in the cloud to connect AWS services and other public or private websites. It provides consistent RESTful APIs for mobile and web applications to access AWS services. In practical terms, API Gateway **(Figure 9)** lets customers create, configure, and host a RESTful API to enable applications to access the AWS Cloud. For example, an application can call an API in API Gateway to upload a user's annual income and expense data to Amazon S3 or Amazon DynamoDB, process the data in AWS Lambda to compute tax owed, and file a tax return via the IRS website.

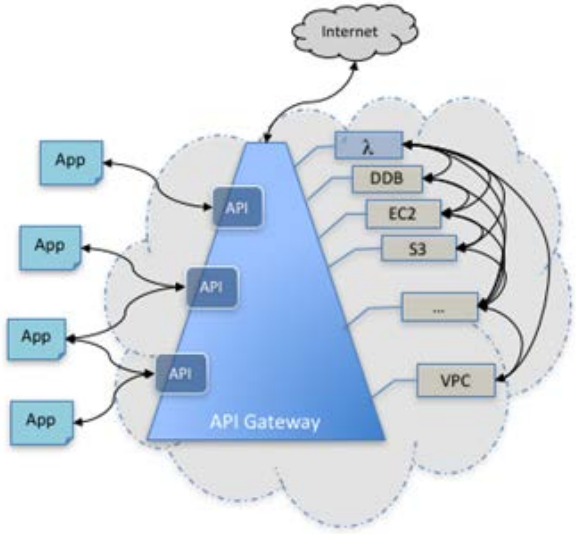


Figure 9 | Standards Based Integration to External Applications and Systems

As shown in the diagram, an app (or client application) gains programmatic access to AWS services, or a website on the internet, through one or more APIs, which are hosted in API Gateway. The app is at the API's frontend. The integrated AWS services and websites are located at the API's backend. In API Gateway, the frontend is encapsulated by method requests and method responses, and the backend is encapsulated by integration requests and integration responses. With Amazon API Gateway, customers can build an API to provide users with an integrated and consistent developer experience to build AWS cloud-based applications.

19.2 Customizing and Personalizing eGT Solutions (8.18.2)

eGT's proposed IaaS and PaaS provider AWS is a highly flexible and configurable solution that can be easily tailored to meet the specific needs of Purchasing Entities. As stated earlier, AWS provides a simple standards-based integration out of the box to integrate with complementary applications and add additional integrations as required. All AWS services including those that fall under the compute, storage, network, security and tools family provide the ability to be configured to meet real-world use case requirements. For instance, the Amazon Machine Image (AMI) that provides the information required to launch virtual compute instances in the cloud, can be completely customized by a Purchasing Entity. A customer or a Purchasing Entity can launch an instance from an existing AMI, customize the instance, and then save this updated configuration as a custom AMI. Instances launched from this new custom AMI include the customizations that a customer made when they created the AMI. Other examples include, the AWS Relational Database Service that can be configured for automatic replication and AWS S3 that can be configured to limit access and privileges to specific groups of users. The AWS Management Console through which services are accessed and configured can be customized and personalized to meet the specific needs of the Purchasing Entity. Individual users of a Purchasing Entity can personalize their digital web experience through a variety of preferences and options available to them. For instance, the AWS Billing and Cost Management Dashboard can be configured with specific billing reports, visualizations and alert notifications that best meet the specific needs of the Purchasing Entity.

20 Marketing Plan (8.19)

Our business development director and marketing manager will work with NASPO to efficiently and effectively market the NASPO Cloud Solutions contract to eligible state and local government institutions. This effort will be tightly integrated into our technology and solutions practice and will involve development of slick-sheets, presentations and case studies that would be part of our overall marketing collateral library. We will work with NASPO to ensure all such materials and campaigns are compliant to any standards and practices instituted by NASPO.

Our marketing manager will work with our business development director, to market the vehicle to all eligible State users. Both will participate in relevant conferences and trade shows to facilitate outreach to State clients, participate in cloud solution discussions, and to identify opportunities to team with other providers of innovative solutions.

eGT professionals regularly attend industry conferences and speak at these forums, owing to our thought leadership. Our experts represent us at these conferences and networking events, and we consider their participation a key part of our marketing strategy.

We will develop a NASPO Cloud Solutions web page to help market the contract. Our marketing manager will update this web portal with current information, including eGT and contract news, advantages of contracting on this vehicle, procedures for placing orders, and our past performance, capabilities, and awards and accolades.

In addition to these activities, we will also leverage our AWS partnership. AWS provides Partner Network (APN) marketing tools which are designed to help AWS partners grow their AWS-based business and reach new customers. We can access the APN self-service tools to market eGT to potential cloud adopters by logging into the APN Portal at any time.

APN Marketing Central. Provides access to self-service marketing campaigns that allow us to quickly co-brand and launch solution-based campaigns or engage participating agencies for select marketing services.

AWS Sponsorships. Sponsorship opportunities allow us to educate, entertain, and engage with the best and the brightest developers and IT decision makers, hottest start-ups, and visionary technology leaders from a wide range of industries.

APN Ho-to Guides. Designed to help us learn best practices to maximize joint marketing efforts with AWS. These guides can be used to extend the skills of our marketing team and help us showcase our services when marketing with AWS.

21 Related Value-Added Services to Cloud Solutions (8.20)

eGT is an IT solutions firm focused on cloud computing, cybersecurity, agile development, DevOps, and the way these disciplines converge on the critical path to IT modernization. eGT has been an early adopter and thought leader in cloud strategies and migration in the Federal space. Working with NIST, eGT helped define Infrastructure-as-a-Service (IaaS) standards including gaining agreement from all 25 cabinet-level agencies for cloud security controls. In 2009 under contract to the GSA, we developed the structure and guidance for the FedRAMP security accreditation for Federal CSPs.

eGT remains at the forefront of Federal cloud computing, offering organizational transformation support services that enable agencies to fully realize the benefits of cloud technologies and business models. We combine the agility and minimal bureaucracy of a midsize firm with the technical expertise gained from migrating a dozen Federal agencies to the cloud. Our cadre of highly certified cloud professionals deliver IaaS, PaaS, and SaaS solutions ranging from strategy and planning through migration and operations.

21.1 Pre- and Post-Implementation Consulting Services

eGT cloud consultants provide services ranging from executive strategy and planning to day-to-day operations and support. We rigorously screen and only hire professionals with top shelf technical chops, proven delivery experience, and excellent customer relationship management skills. Our employees quickly become our customer’s "go to" person on the projects they support.

Cloud Strategy and Planning. Cloud-savvy eGT Business Analysts develop comprehensive IT portfolio needs analysis, enterprise cloud strategies, and acquisition guidelines and standards. We evaluate investments to determine viability for cloud deployment and perform total cost of ownership and technical analyses to determine optimal migration strategies.

Cloud Environment Provisioning. Our Managed Cloud Services team will use automation tools and processes to provision and operationalize cloud environments. We will bake in security controls, instrument monitoring and sufficiently configure the platforms to simplify on-boarding of customer workloads

Cloud Migration. Certified eGT Cloud Solution Architects identify the right CSP and service mix and create a smooth migration process for infrastructure, platforms, and applications. Developers roll out initial proofs of concept to mitigate risk. DevOps Engineers orchestrate immutable infrastructure deployments using open source infrastructure-as-code tools to maximize operational efficiency.

Cloud Security. eGT DevOps Engineers bake security monitoring tools into system orchestration, enabling rapid system teardown and rebuild responses to intrusions. Certified Information System Security Officers (ISSOs) evaluate CSP security authorization packages (SSP, SAP, SAR, Policies, and Procedures), architectures, and vulnerabilities, and specify recommendations to obtain successful authorization to operate within the organizations infrastructure. ISSOs review scans and resulting vulnerability management plans and identify CSPs not meeting pre-established SLAs, or not remediating Plans of Action and Milestones (POA&Ms) within established time limits.

Managed Cloud Operations & Maintenance.

Post-implementation and migration of workloads to our recommended AWS cloud platform, we offer customers managed cloud O&M services. This includes providing system administration, log aggregation and management, system patching, security monitoring and site reliability engineering services. Through several years of providing such services to agencies such as FEMA and HHS, we have matured our automated tools and processes optimizing cost and maximizing value for our customers.

21.2 Professional Services

eGT's cloud focused professional services offerings have been detailed in the previous **Section 21.1 Pre and Post Implementation Services**. In the process of migrating agencies and applications to the cloud, eGT developed and trademarked a framework of the most effective migration processes and best-of-breed open source cloud automation technologies—the eGT DevOps Factory® (**Figure 1**). DevOps Factory is our full featured, foundational platform used to execute the service offerings under our Technology Solutions Practice including cloud enablement and migration services. We provide comprehensive cloud adoption and implementation services spanning beyond conventional models, such as IaaS, PaaS, or SaaS, and focus on enabling Anything as-a Service (XaaS). We maximize the agility and cost efficiencies offered by cloud platforms by automating and orchestrating the entire application stack inclusive of software deployment, network configuration, security controls, and system monitoring. By applying techniques such as "Infrastructure as Code," "Composable Service Architecture," and Containerization, we simplify and streamline the entire cloud transformation process. We leverage industry leading tools such as Chef, Puppet, Ansible, Docker, and our own Cloudamatic® to accelerate complex cloud migration and implementation initiatives saving both time and money for our clients. Our services include:

- Cloud Assessment, Planning, and Architecture
- Cloud Migration and Transformation
- Cloud Operations
- Managed Cloud Services

22 Supporting Infrastructure (8.22)

The Supporting infrastructure will be hosted and provided by AWS. eGT will support the deployment and migrations of the systems and applications to the AWS infrastructure and support the operations of it.

22.1 Required Purchasing Entity Infrastructure (8.22.1)

The IaaS solution will not require the purchasing of new infrastructure as it will be provided by the IaaS provider unless otherwise specified based on networking requirements related to VPN or dedication connections.

22.2 Installation of New Infrastructure (8.22.2)

The IaaS solution will not require any hardware installation. The requirements to establish connectivity to the existing data centers will detail any procurements. If a physical firewall is required to be established, AWS Direct Connect can do so through most co-location providers such as Equinix Cloud Exchange. Any procurements that arise will be procured by the Purchasing Entity and eGT will support the installation as applicable including the configurations and testing.

Last Updated March 14, 2019

This Amazon CloudFront Service Level Agreement ("**SLA**") is a policy governing the use of Amazon CloudFront under the terms of the Amazon Web Services Customer Agreement (the "**AWS Agreement**") between Amazon Web Services, Inc. and its affiliates ("**AWS**", "**us**" or "**we**") and users of AWS' services ("**you**"). This SLA applies separately to each account using Amazon CloudFront. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement

Service Commitment

AWS will use commercially reasonable efforts to make Amazon CloudFront available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the "**Service Commitment**"). In the event Amazon CloudFront does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "**Error Rate**" means: (i) the total number of internal server errors returned by Amazon CloudFront divided by (ii) the total number of requests during that five minute period. We will calculate the Error Rate for each Amazon CloudFront account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon CloudFront SLA Exclusions (as defined below).

Less than 99.0% but greater than or equal to 95.0%	25%
Less than 95.0%	100%

We will apply any Service Credits only against future Amazon CloudFront payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon CloudFront is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words "**SLA Credit Request**" in the subject line;

ii. the dates and times of each incident of non-zero Error Rates that you are claiming; and

iii. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

than Amazon S3 (collectively, the "**Amazon CloudFront SLA Exclusions**"). If availability is impacted by factors other than those used in our calculation of the Error Rate, then we may issue a Service Credit considering such factors at our discretion.

Prior Version(s): Link

Discover how to get started with Amazon CloudFront for free

Visit the getting started page

Ready to build?

Get started with Amazon CloudFront

Have more questions?

Contact us

AWS NEWS BLOG

Latest new products and features announced at AWS Summit Santa Clara

Amazon CloudFront

- Overview
- Features
- Pricing
- Getting Started
- Resources
- FAQs
- Case Studies

Twitter Facebook Podcast Twitch AWS Blog RSS News Feed
Email Updates

AWS & Cloud Computing

What is Cloud Computing?
What is Caching?
What is NoSQL?
What is DevOps?
What is Docker?
Products & Services
Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal
UK Modern Slavery Statement

Solutions

Websites & Website Hosting

Amazon CloudFront

- Overview
- Features
- Pricing
- Getting Started
- Resources
- FAQs
- Case Studies

Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account

Management Console

Amazon CloudFront

- Overview
- Features
- Pricing
- Getting Started
- Resources
- FAQs
- Case Studies

Amazon Compute Service Level Agreement

Last Updated: March 19, 2019

This Amazon Compute Service Level Agreement (this "SLA") is a policy governing the use of the Included Services (listed below) and applies separately to each account using the Included Services. In the event of a conflict between the terms of this SLA and the terms of the AWS Customer Agreement or other agreement with us governing your use of our Services (the "Agreement"), the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

Included Services

- Amazon Elastic Compute Cloud (Amazon EC2)*
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Fargate for Amazon ECS (Amazon Fargate)

*For purposes of this SLA, Amazon EC2 includes any Amazon Elastic Graphics, Amazon Elastic Inference, and Elastic IP Address resources purchased with the relevant Amazon EC2 instance(s).

General Service Commitment

AWS will use commercially reasonable efforts to make the Included Services each available for each AWS region with a Monthly Uptime Percentage of at least 99.99%, in each case during any monthly billing cycle (the "Service Commitment"). In the event any of the Included Services do not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Service Credits

AWS region for the monthly billing cycle in which the Unavailability occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	30%
Less than 95.0%	100%

We will apply any Service Credits only against future payments for the applicable Included Service otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Unavailability occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

1. the words “SLA Credit Request” in the subject line;

2. the dates, times, and affected AWS region of each Unavailability incident that you are claiming;

3. the resource IDs for the affected Included Service ; and

4. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit. Unless otherwise provided in the Agreement, this SLA sets forth your sole and exclusive remedies, and AWS' sole and exclusive obligations, for any unavailability, non-performance, or other failure by us to provide the Included Services.

Single EC2 Instances

AWS will use commercially reasonable efforts to ensure that each individual Amazon EC2 instance ("Single EC2 Instance") has an Hourly Uptime Percentage of at least 90% of the time in which that Single EC2 Instance is deployed during each clock hour (the "Hourly Commitment"). In the event any Single EC2 Instance does not meet the Hourly Commitment, you will not be charged for that instance hour of Single EC2 Instance usage.

Amazon Compute SLA Exclusions

The Service Commitment and Hourly Commitment do not apply to any unavailability, suspension or termination an Included Service, or any other Included Service performance issues: (i) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of the applicable Included Service; (ii) that result from any actions or inactions of you or any third party, including failure to acknowledge a recovery volume; (iii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (iv) arising from our suspension or termination of your right to use the applicable Included Service in accordance with the Agreement (collectively, the "Amazon Compute SLA Exclusions"). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

Definitions

• "Availability Zone" and "AZ" mean an isolated location within an AWS region identified by a letter identifier following the AWS region code (e.g., us-west-1a).

• "Hourly Uptime Percentage" is calculated by subtracting from 100% the percentage of deployed minutes during any clock hour in which a Single EC2 Instance was in a state of Unavailability. Hourly Uptime Percentage measurements exclude Unavailability resulting directly or indirectly from any Amazon Compute SLA Exclusion

• "Monthly Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during the month in which any of the Included Services, as applicable, was in the state of Unavailability. Monthly Uptime Percentage measurements exclude Unavailability resulting directly or indirectly from any Amazon Compute SLA Exclusion.

• A "Service Credit" is a dollar credit, calculated as set forth above, that we may credit back to an eligible account.

o For Single EC2 Instances, when your Single EC2 Instance has no external connectivity.
o For Amazon EC2 (other than Single EC2 Instances), Amazon ECS, or Amazon Fargate, when all of your running instances or running tasks, as applicable, deployed in two or more AZs in the same AWS region (or, if there is only one AZ in the AWS region, that AZ and an AZ in another AWS region) concurrently have no external connectivity.
o For Amazon EBS, when all of your attached volumes deployed in two or more AZs in the same AWS region (or, if there is only one AZ in the AWS region, that AZ and an AZ in another AWS region) perform zero read write IO, with pending IO in the queue.

Prior Version(s): Link

Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon is an Equal Opportunity Employer – Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Tiếng Việt | Türkçe | Русский | ไทย | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy

Amazon RDS Service Level Agreement

Last Updated: March 21, 2019

This Amazon RDS Service Level Agreement ("SLA") is a policy governing the use of the Amazon Relational Database Service ("Amazon RDS") and applies separately to each account using Amazon RDS. In the event of a conflict between the terms of this SLA and the terms of the AWS Customer Agreement or other agreement with us governing your use of our Services (the "Agreement"), the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Multi-AZ instances available with a Monthly Uptime Percentage of at least 99.95% during any monthly billing cycle (the "Service Commitment"). In the event Amazon RDS does not meet the Monthly Uptime Percentage commitment, you will be eligible to receive a Service Credit as described below.

Service Credits

Service Credits are calculated as a percentage of the charges paid by you for the Multi-AZ instances that did not meet the Monthly Uptime Percentage commitment in a billing cycle in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

We will apply any Service Credits only against future Amazon RDS payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the unavailability occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Agreement, your sole and exclusive remedy for any unavailability or non-performance or other failure by us to provide Amazon RDS is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you will need to submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words "SLA Credit Request" in the subject line;

ii. the dates and times of each Unavailability incident you are claiming;

iii. the DB Instance IDs and the AWS regions of the affected Multi-AZ instances; and

iv. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which the request occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon RDS SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon RDS, or any other Amazon RDS performance issues: (i) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon RDS; (ii) that result from any voluntary actions or inactions from you or any third party; (iii) that result from instances belonging to the Micro DB instance class or other instance classes which have similar CPU and memory resource limitations; (iv) that result from you not following the basic operational guidelines described in the Amazon RDS User Guide (e.g., overloading a database instance to the point it is inoperable, creating excessively large number of tables that significantly increase the recovery time etc.); (v) caused by underlying database engine software that lead to repeated database crashes or an inoperable database instance; (vi) that result in long recovery time due to insufficient IO capacity for your database workload; (vii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (viii) that result from any maintenance as

If availability is impacted by factors other than those explicitly used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

Definitions

- "Monthly Uptime Percentage" for a given Multi-AZ instance is calculated by subtracting from 100% the percentage of 1 minute intervals during the monthly billing cycle in which the Multi-AZ instance was "Unavailable". If you have been running that Multi-AZ instance for only part of the month, your Multi-AZ instance is assumed to be 100% available for the portion of the month that it was not running. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon RDS SLA Exclusion.
- "Multi-AZ instance" means an Amazon RDS for MySQL, MariaDB, Oracle, PostgreSQL, or SQL Server database instance with the Multi-AZ parameter set to true.
- A "Service Credit" is a dollar credit, calculated as set forth above, that we may credit back to an eligible account.
- "Unavailable" means that all connection requests to the running Multi-AZ instance fail during a 1 minute interval.

Prior Version(s)

AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal
UK Modern Slavery Statement

Solutions

Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS

User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account

Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon is an Equal Opportunity Employer – Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Tiếng Việt | Türkçe | Русский | ไทย | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy

Amazon Route 53 Service Level Agreement

Last Updated November 21, 2018

This Amazon Route 53 Service Level Agreement ("**SLA**") is a policy governing the use of Amazon Route 53 (including Private DNS) under the terms of the Amazon Web Services Customer Agreement (the "**AWS Agreement**") between Amazon Web Services, Inc. and its affiliates ("**AWS**", "**us**" or "**we**") and users of AWS' services ("**you**"). This SLA applies separately to each account using Amazon Route 53. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon Route 53 100% Available (defined below). In the event Amazon Route 53 does not meet the foregoing commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "**100% Available**" means that Amazon Route 53 did not fail to respond to your DNS queries during a monthly billing cycle.
- A "**Service Credit**" is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon Route 53 account.

Service Credits

Service Credits are calculated based on 1 day of Service Credit, which is equal to your average daily Amazon Route 53 query charges for the monthly billing cycle preceding the monthly billing cycle in which the period that Amazon Route 53 was not 100% Available occurred, and are available as follows:

Duration Amazon Route 53 was not 100% Available	Service Credit
5 - 30 minutes	1 day Service Credit

More than 4 hours	30 days Service Credit

We will apply any Service Credits only against future Amazon Route 53 payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon Route 53 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words “SLA Credit Request” in the subject line;

ii. the dates and times of each period that Amazon Route 53 was not 100% Available that you are claiming; and

iii. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the period that Amazon Route 53 was not 100% Available is confirmed by us, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon Route 53 SLA Exclusions

The Service Commitment does not apply to (a) the Route 53 Resolver service or (b) any unavailability, suspension or termination of Amazon Route 53, or any other Amazon Route 53 performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon Route 53; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension

public DNS only, result during a period that you were not using all four virtual name servers (for example, ns123.awsdns.com, ns123.awsdns.net, ns123.awsdns.co.uk and ns123.awsdns.org) assigned to your "hosted zone" (collectively, the "**Amazon Route 53 SLA Exclusions**"). If availability is impacted by factors other than those used in our calculation of 100% Available, then we may issue a Service Credit considering such factors at our discretion.

Prior Version(s)

Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account

Management Console
Billing & Cost Management

Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon is an Equal Opportunity Employer – Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.

Amazon S3 Service Level Agreement

Last Updated: March 20, 2019

This Amazon S3 Service Level Agreement ("SLA") is a policy governing the use of Amazon S3 and Amazon S3 Glacier (each an "Amazon S3 Service") and applies separately to each account using an Amazon S3 Service. In the event of a conflict between the terms of this SLA and the terms of the AWS Customer Agreement or other agreement with us governing your use of our Services (the "Agreement"), the terms and conditions of this SLA apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make the Amazon S3 Services each available with a Monthly Uptime Percentage, as described below, during any monthly billing cycle (the "Service Commitment"). In the event an Amazon S3 Service does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for the applicable Amazon S3 Service in the AWS region affected for the billing cycle in which the Monthly Uptime Percentage fell within the ranges set forth in the table below.

For all requests not otherwise specified below:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.9% but greater than or equal to 99.0%	10%
Less than 99.0% but greater than or equal to 95.0%	25%

For requests to S3 Intelligent-Tiering, S3 Standard-Infrequent Access, and S3 One Zone-Infrequent Access:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.9% but greater than or equal to 98.0%	10%
Less than 98.0% but greater than or equal to 95.0%	25%
Less than 95.0%	100%

We will apply any Service Credits only against future payments otherwise due from you for the Amazon S3 Service. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Amazon S3 Service did not meet the Service Commitment. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Amazon S3 Services is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

1. the words “SLA Credit Request” in the subject line;

2. the billing cycle and AWS region with respect to which you are claiming Service Credits together with the dates and times of each incident of non-zero Error Rates that you are claiming; and

3. your request logs that document claimed incident(s) when the Amazon S3 Service did not meet the Service Commitment (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than the applicable Service Commitment, then we will issue the Service Credit to you within one billing cycle

Amazon S3 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of an Amazon S3 Service, or any other Amazon S3 Service performance issues: (i) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of the Amazon S3 Service; (ii) that result from any actions or inactions of you or any third party; (iii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (iv) arising from our suspension or termination of your right to use the Amazon S3 Service in accordance with the AWS Agreement (collectively, the "Amazon S3 SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of the Monthly Uptime Percentage, then we may issue a Service Credit considering such factors at our discretion.

Definitions

• "Error Rate" means: (i) the total number of internal server errors returned by the Amazon S3 Service as error status "InternalError" or "ServiceUnavailable" divided by (ii) the total number of requests for the applicable request type during that 5-minute interval. We will calculate the Error Rate for each Amazon S3 Service account as a percentage for each 5-minute interval in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon S3 SLA Exclusions.

• "Monthly Uptime Percentage" is calculated by subtracting from 100% the average of the Error Rates from each 5-minute interval in the monthly billing cycle. If you did not make any requests in a given 5-minute interval, that interval is assumed to have a 0% Error Rate.

• A "Service Credit" is a dollar credit, calculated as set forth above, that we may credit back to an eligible Amazon S3 Service account.

Previous version(s)

What is NoSQL?
What is DevOps?
What is Docker?
Products & Services
Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal
UK Modern Slavery Statement

Solutions

Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account

Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon is an Equal Opportunity Employer – Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.

AWS Service Terms

Last Updated: March 20, 2019

The following Service Terms apply only to the specific Services to which the Service Terms relate. In the event of a conflict between the terms of these Service Terms and the terms of the AWS Customer Agreement or other agreement with us governing your use of our Services (the **"Agreement"**), the terms and conditions of these Service Terms apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

1. Universal Service Terms (Applicable to All Services)

1.1. You may only use the Services to store, retrieve, query, serve, and execute Your Content that is owned, licensed or lawfully obtained by you. As used in these Service Terms, (a) "Your Content" includes any "Company Content" and any "Customer Content" and (b) "AWS Content" includes "Amazon Properties". As part of the Services, you may be allowed to use certain software (including related documentation) provided by us or third party licensors. This software is neither sold nor distributed to you and you may use it solely as part of the Services. You may not transfer it outside the Services without specific authorization to do so.

1.2. You must comply with the current technical documentation applicable to the Services (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site. In addition, if you create technology that works with a Service, you must comply with the current technical documentation applicable to that Service (including the applicable developer guides) as posted by us and updated by us from time to time on the AWS Site.

1.3. You will provide information or other materials related to Your Content (including copies of any client-side applications) as reasonably requested by us to verify your compliance with the Agreement. We may monitor the external interfaces (e.g., ports) of Your Content to verify your compliance with the Agreement. You will not block or interfere with our monitoring, but you may use encryption technology or firewalls to help keep Your Content confidential. You will reasonably cooperate with us to identify the source of any problem with the Services that we reasonably believe may be attributable to Your Content or any end user materials that you control.

1.4. If we reasonably believe any of Your Content violates the law, infringes or misappropriates the rights of any third party or otherwise violates a material term of the Agreement (including the documentation, the Service Terms, or the Acceptable Use Policy) ("Prohibited Content"), we will notify you of the Prohibited

or disable access to the Prohibited Content or suspend the Services to the extent we are not able to remove or disable access to the Prohibited Content. Notwithstanding the foregoing, we may remove or disable access to any Prohibited Content without prior notice in connection with illegal content, where the content may disrupt or threaten the Services, pursuant to the Digital Millennium Copyright Act or as required to comply with law or any judicial, regulatory or other governmental order or request. In the event that we remove content without prior notice, we will provide prompt notice to you unless prohibited by law.

1.5. From time to time, we may offer free or discounted pricing programs covering certain usage of the Services (each, a "Special Pricing Program"). We may stop accepting new sign-ups or discontinue a Special Pricing Program at any time. Standard charges will apply after a Special Pricing Program ends or if you exceed the limitations by the Special Pricing Program. You must comply with any additional terms, restrictions, or limitations (e.g., limitations on the total amount of usage) for the Special Pricing Program as described in the offer terms for the Special Pricing Program or on the pricing page for the eligible Service(s). You may not access or use the Services in a way intended to avoid any additional terms, restrictions, or limitations (e.g., establishing multiple AWS accounts in order to receive additional benefits under a Special Pricing Program), and we may immediately terminate your account if you do so. Any data stored or instances provided as part of a Special Pricing Program must be actively used.

1.6. If we make multiple discounts or pricing options for a Service available to you at one time, you will only be eligible to receive one discount or pricing option, and will not be entitled to cumulative discounting and pricing options.

1.7. You will ensure that all information you provide to us via the AWS Site (for instance, information provided in connection with your registration for the Services, requests for increased usage limits, etc.) is accurate, complete and not misleading.
1.8. From time to time, we may apply upgrades, patches, bug fixes or other maintenance to the Service Offerings ("Maintenance"). We agree to use reasonable efforts to provide you with prior notice of any scheduled Maintenance (except for emergency Maintenance) and you agree to use reasonable efforts to comply with any Maintenance requirements that we notify you about.

1.9. If your Agreement does not include a provision on AWS Confidential Information, and you and AWS do not have an effective non-disclosure agreement in place, then you agree that you will not disclose AWS Confidential Information (as defined in the AWS Customer Agreement), except as required by law.

1.10. Beta Service Participation

1.10.1. This Section describes the additional terms and conditions under which you may access and use certain features, technologies and services made available to you by AWS that are not yet generally available, including, but not limited to, any products, services, or features labeled "beta", "preview", "pre-release", or "experimental" (each, a "Beta Service") or access and use Service Offerings available in AWS regions that are not generally available, including, but not limited to, any AWS regions identified by AWS as "beta", "preview", "pre-release", or "experimental" (each, a "Beta Region"). In the event there is a conflict between the terms of

1.10.2. During the term of the applicable Beta Service or Beta Region (as specified by AWS), you may: (a) access and use the Beta Service or Service Offerings in any Beta Region solely for internal evaluation purposes; and (b) install, copy, and use any related AWS Content that may be provided to you by AWS in connection with the Beta Service or Service Offerings in any Beta Region ("Beta Materials") solely as necessary to access and use the Beta Service or Service Offerings in any Beta Region in the manner permitted by this Section.

1.10.3. You agree not to allow access to or use of any Beta Service, Service Offerings in any Beta Region or Beta Materials by any third party other than your employees and contractors who (i) have a need to use or access the Beta Service, Service Offerings in the Beta Region or Beta Materials in connection with your internal evaluation activities, and (ii) have executed written non-disclosure agreements obligating them to protect the confidentiality of non-public information regarding the Beta Service, Beta Region and Beta Materials.

1.10.4. You must comply with all policies and guidelines related to any Beta Service or Beta Region as posted on the AWS Site or otherwise made available to you, including the Privacy Policy, Acceptable Use Policy, the Service Terms, and any additional terms and conditions for a specific Beta Service or Beta Region. AWS may add or modify restrictions, including lowering or raising any usage limits, related to access to or use of any Beta Service, Service Offerings in any Beta Region or Beta Materials at any time. If requested by AWS, you will promptly increase or decrease your usage of the applicable Beta Service, Service Offerings in a Beta Region or Beta Materials to the levels that AWS may specify. Service Level Agreements do not apply to Beta Services or any Services Offerings in Beta Regions.

1.10.5. AWS may suspend or terminate your access to or use of any Beta Service or Service Offerings in any Beta Region at any time and for any reason. AWS may at any time cease providing any or all of any Beta Service or any Service Offering in a Beta Region in its sole discretion and without notice. Beta Services and Services Offerings in Beta Regions also may be unavailable and/or their performance may be negatively affected by scheduled and unscheduled maintenance. AWS will use reasonable efforts to notify you in advance of scheduled maintenance, but AWS is unable to provide advance notice of unscheduled or emergency maintenance.

1.10.6. In consideration of being allowed to access and use a Beta Service or Service Offering in a Beta Region, you agree to provide AWS with information relating to your access, use, testing, or evaluation of the Beta Service, Service Offerings in the Beta Region or any related Beta Materials, including observations or information regarding the performance, features and functionality of the Beta Service or any related Beta Materials as applicable, when and in the form reasonably requested by AWS ("Test Observations"). AWS will own and may use and evaluate all Test Observations for its own purposes. You will not use any Test Observations except for your internal evaluation purposes of the Beta Service or Beta Region.

1.10.7. Each individual Beta Service and Service Offering in a Beta Region will automatically terminate upon the release of a generally available version of the applicable Beta Service or Service Offering in a Beta Region or upon notice of termination by AWS. Notwithstanding anything to the contrary in the Agreement or these Services Terms, either you or AWS may terminate your participation in a Beta Service or Service Offering in a Beta Region at any time for any reason upon notice to the other party. Notwithstanding anything to the

or Service Offering in the Beta Region and Beta Materials; (b) your Content used in the applicable Beta Service or Service Offering in the Beta Region may be deleted or inaccessible; and (c) you will immediately return or, if instructed by AWS, destroy all Beta Materials or any other AWS Confidential Information related to the applicable Beta Service, Service Offering in any Beta Region or Beta Materials. If AWS releases a generally available version of a Beta Service or a Service Offering in a Beta Region, your access to and use of the generally available version will be subject to the Agreement and any separate Section of these Service Terms as may be specified for that generally available Service Offering. If any Beta Region becomes generally available, your access to and use of Service Offerings in the generally available AWS region will be subject to the terms and conditions applicable to that AWS region. AWS does not guarantee that any Beta Service or Service Offering in any Beta Region will ever be made generally available, or that any generally available version will contain the same or similar functionality as the version made available by AWS during the term of the Beta Service or Beta Region, as applicable. AWS does not guarantee that any Beta Region will become generally available.

1.10.8. Beta Materials, Test Observations, Suggestions concerning a Beta Service or Beta Region, or any other information about or involving (including the existence of) any Beta Service or Beta Region are considered AWS Confidential Information. You will not disclose (including, but not limited to, in a press release or public statement) any Beta Materials, Test Observations, Suggestions concerning a Beta Service, or any other information about or involving (including the existence of) any Beta Service, except as agreed by AWS in writing.

1.10.9. ADDITIONAL WARRANTY DISCLAIMERS. WITHOUT LIMITING ANY DISCLAIMERS IN THE AGREEMENT OR THE SERVICE TERMS, THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS ARE NOT READY FOR GENERAL COMMERCIAL RELEASE AND MAY CONTAIN BUGS, ERRORS, DEFECTS OR HARMFUL COMPONENTS. ACCORDINGLY, AND NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE AGREEMENT OR THESE SERVICES TERMS, AWS IS PROVIDING THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS AND BETA MATERIALS TO YOU "AS IS." AWS AND ITS AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS, INCLUDING ANY WARRANTY THAT THE BETA SERVICES, SERVICE OFFERINGS IN BETA REGIONS, BETA REGIONS AND BETA MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, AWS AND ITS AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE. AWS' AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY FOR ANY BETA SERVICES WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE BETA SERVICES THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

1.10.10. Because the Beta Services and Materials involve features, technologies and services that are not yet generally available, you acknowledge that any violation of this Section 1.10 could cause irreparable harm to

violation of this Section 1.10.

1.11. You may perform benchmarks or comparative tests or evaluations (each, a "Benchmark") of the Service Offerings. If you perform or disclose, or direct or permit any third party to perform or disclose, any Benchmark of any of the Service Offerings, you (i) will include in any disclosure, and will disclose to us, all information necessary to replicate such Benchmark, and (ii) agree that we may perform and disclose the results of Benchmarks of your products or services, irrespective of any restrictions on Benchmarks in the terms governing your products or services.

1.12. Only the applicable AWS Contracting Party (as defined in the AWS Customer Agreement) will have obligations with respect to each AWS account, and no other AWS Contracting Party has any obligation with respect to such account. The AWS Contracting Party for an account may change as described in the Agreement. Invoices for each account will reflect the AWS Contracting Party that is responsible for that account during the applicable billing period.

If, as of the time of a change of the AWS Contracting Party responsible for your account, you have made an up-front payment for any EC2 Reserved Instances, Reserved DB Instances, Reserved Cache Nodes, Amazon DynamoDB Reserved Capacity, or Reserved Nodes (each as defined in these Service Terms for the applicable Service) under such account, then the AWS Contracting Party you paid such up-front payment to will remain the AWS Contracting Party for the applicable account only with respect to the Services related to such up-front payment.

1.13. If you are a customer that is subject to the French Politique générale de sécurité des systems d'information de santé (PGSSI-S), you agree that your use of AWS Offerings complies with the PGSSI-S.

2. Amazon CloudFront

2.1. You must own or have all necessary rights to use any domain name or SSL certificate that you use in conjunction with Amazon CloudFront. You are solely responsible for the renewal, security and proper configuration of any SSL certificates that you provide for use with Amazon CloudFront, including any disclosure of your SSL certificates to third parties.

2.2. Amazon CloudFront requires you to store the original version of Your Content in an origin server (such as Amazon S3). If you use other Services to store the original version of Your Content, you are responsible for the separate fees you accrue for the other Services and for Amazon CloudFront.

2.3. While you will only be charged fees specified for the selected Price Class, Your Content you select for delivery from edge locations in a Price Class may from time to time be served from edge locations located outside the regions in that Price Class.

2.4. Amazon CloudFront's Geo Restriction feature may utilize a third party geo-location database, which may not be accurate in all situations.

3.1. You may not knowingly create and maintain inactive queues. We may delete, without liability of any kind, any of Your Content that sits in an Amazon SQS queue or any Amazon SQS queue that remains inactive for more than the number of days specified in the user documentation.

4. Amazon Elastic Compute Cloud

4.1. In connection with your use of Amazon Elastic Compute Cloud (including all instances and instance types, hosts and other resources, dedicated, reserved or on-demand, collectively "Amazon EC2") and the Services, you are responsible for maintaining licenses and adhering to the license terms of any software you run.

4.2. Using Microsoft Software. In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the "Microsoft Software").

4.2.1. If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

- The Microsoft Software is neither sold nor distributed to you and you may use it solely in conjunction with the Services.
- You may not transfer or use the Microsoft Software outside the Services.
- You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Software.
- You may not reverse engineer, decompile or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.
- Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.
- You are not granted any right to use the Microsoft Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, **"High Risk Use"**). Microsoft and its suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.
- Microsoft is an intended third-party beneficiary of this Section 4.2.1, with the right to enforce its provisions.

running within the Microsoft Instance, unless (a) you are the ultimate end user of the Microsoft Instance, (b) you have supplemented the Microsoft Instance with your own applications, or (c) you have added primary and significant functionality to the Microsoft Instance.

4.3. Using Third Party Software. In conjunction with the Services, you may be allowed to use certain software (including related support, maintenance, and documentation) developed, owned or provided by third parties or their licensors. Use of third party software is subject to these additional terms and conditions:

- By using NVIDIA Corporation's GRID Software, you agree to be bound by the terms and conditions of the NVIDIA GRID Cloud End User License Agreement located at http://aws-nvidia-license-agreement.s3.amazonaws.com/NvidiaGridAWSUserLicenseAgreement.DOCX.
- By using NVIDIA Corporation's Tesla Driver, CUDA Toolkit, cuDNN, NVENC, NVCUVID, NVM:, nvidia-smi, and NCCL Library Software, toolkits, and drivers, you agree to be bound by the terms and conditions of the NVIDIA Cloud End User License Agreement located at https://s3.amazonaws.com/EULA/Nvidia-EULA.txt and NVIDIA Third Party Materials Notices located at https://s3.amazonaws.com/EULA/Nvidia-3P-Notice.txt.
- By using Red Hat, Inc.'s software, you agree to be bound by the terms and conditions of the Red Hat Cloud Software Subscription Agreement located at www.redhat.com/licenses/cloud_cssa/. Red Hat also disclaims any (i) warranties with respect to Red Hat, Inc. software; and (ii) liability for any damages, whether direct, indirect, incidental, special, punitive or consequential, and any loss of profits, revenue, data or data use, arising from use of Red Hat, Inc. software.
- By using SUSE LLC's software, you agree to be bound by the terms and conditions of the SUSE End User License Agreement located at https://www.suse.com/licensing/eula and the SUSE Terms and Conditions located at https://www.suse.com/products/terms_and_conditions.pdf.

4.4. Spot Instance Pricing. You may request that certain Amazon EC2 instances run pursuant to the Spot instance pricing and payment terms ("Spot Instance Pricing") set forth on the Amazon EC2 product detail page on the AWS Site (each requested instance, a "Spot Instance"). You must request Spot Instances through the AWS Management Console or by using API tools ("Spot Instance Request"). As part of your Spot Instance Request, you may specify the maximum hourly price you are willing to pay to run the requested Spot Instances ("Your Maximum Price"). Unless you specify a permissible alternative termination date, your Spot Instance Request will remain active until the earlier of the following: (1) seven (7) days have passed, (2) we fulfill it, or (3) you cancel it. We set the price for Spot Instances (the "Spot Price"), which may vary over time based on a number of factors, including the amount of available compute capacity we have available and the price you and other customers are willing to pay for Spot Instances (e.g., supply and demand). While a requested Spot Instance remains running, you will be charged the current Spot Price in effect at the beginning of each instance hour. If you have specified Your Maximum Price, then you will not be charged more than Your Maximum Price. We may terminate, stop, or hibernate Spot Instances at any time and without any notice to you if we determine the current Spot Price equals or exceeds Your Maximum Price (if specified) or for AWS capacity requirements. If we terminate, stop, or hibernate your Spot Instance, you will be charged as described on the Amazon EC2 product detail page on the AWS Site. AWS may allow you to purchase Spot Instances of a fixed duration (each, a "Spot Block"), where the Spot Price for that Spot Instance (the "Block Price") will

terminated because the Spot Price equals or exceeds Your Maximum Price (if specified). Spot Instances purchased as Spot Blocks may still be terminated for AWS capacity requirements and will terminate at the conclusion of the fixed duration. If a Spot Instance purchased as a Spot Block is terminated due to AWS capacity requirements, you will not be charged for that Spot Instance. Unless you designate your Spot Instance Request as a persistent request, terminated, stopped or hibernated Spot Instances may not automatically restart. You should save your work frequently and test your application to ensure it is fault tolerant and will correctly handle interruptions. We have no liability whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from our termination, stoppage, or hibernation of any Spot Instance. Spot Instances may not be used with certain Services, features and third-party software we specify, including Amazon DevPay, IBM software packages, or Microsoft SQL Server. You may not, directly, indirectly, alone or in cooperation with any third party, attempt to control, influence or manipulate the price for Spot Instances. Without limiting the foregoing, you may not submit requests for Spot Instances through any third party (e.g., "proxy bidding") or share information with any third party regarding the maximum prices specified in your Spot Instance Requests. We may modify or terminate the Spot Instance Pricing program at any time. In addition to the Spot Instance Pricing, Spot Instances are subject to all data transfer and other usage fees applicable under the Agreement.

4.5. EC2 Reserved Instance Pricing. You may designate Amazon EC2 instances as subject to the reserved pricing and payment terms (**"EC2 Reserved Instance Pricing"**) set forth on the Amazon EC2 detail page on the AWS Site (each designated instance, an **"EC2 Reserved Instance"**). Scheduled EC2 Reserved Instances (**"Scheduled Instances"**) will terminate upon completion of the scheduled reservation. You may designate instances as EC2 Reserved Instances by calling to the Purchasing API or selecting the EC2 Reserved Instance option in the AWS console. The EC2 Reserved Instances may only be used in the applicable AWS region. We may change EC2 Reserved Instance Pricing at any time but price changes will not apply to previously designated EC2 Reserved Instances, except as described in this Section 4.5. If Microsoft increases the license fees it charges for Windows, or if Red Hat increases the license fees it charges for Red Hat Enterprise Linux (**"RHEL"**), we may make a corresponding increase to the per-hour usage rate (or institute a corresponding per-hour usage rate) for EC2 Reserved Instances with Windows or RHEL. Any increase in (or institution of) the per-hour usage rate for EC2 Reserved Instances with Windows will be made between December 1 and January 31, and we will provide 30 days' notice. For any increase in (or institution of) the per-hour usage rate for EC2 Reserved Instances with RHEL we will provide 30 days' notice. If this happens, you may: (a) continue to use your EC2 Reserved Instances with Windows or RHEL with the new per-hour usage price; (b) convert your EC2 Reserved Instances with Windows or RHEL to comparable EC2 Reserved Instances with Linux; or (c) terminate your EC2 Reserved Instances with Windows or RHEL and receive a pro rata refund of the up-front fee you paid for the terminated EC2 Reserved Instances with Windows or RHEL. We may terminate the EC2 Reserved Instance Pricing program at any time. EC2 Reserved Instances are nontransferable, except in accordance with the requirements of the RI Marketplace, but Scheduled Instances and Convertible Reserved Instances (as defined on Amazon EC2 detail page on the AWS Site) are not eligible for the RI Marketplace. EC2 Reserved Instances are noncancellable and you will owe the EC2 Reserved Instance Pricing for the duration of the term you selected, even if the Agreement is terminated. All amounts paid in connection with the EC2 Reserved Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an

Instances. You may not purchase EC2 Reserved Instances for the purpose of reselling them in the RI Marketplace, and we reserve the right to refuse or cancel your purchase if we suspect you are doing so. Upon expiration or termination of the term of EC2 Reserved Instances, the EC2 Reserved Instance pricing will expire and standard on-demand usage prices will apply to the instances. In addition to being subject to EC2 Reserved Instance Pricing, EC2 Reserved Instances are subject to all data transfer and other fees applicable under the Agreement.

4.6. EC2 Reserved Instance (RI) Marketplace.

4.6.1. Eligibility. The rights to an active EC2 Reserved Instance can be offered for sale through the RI Marketplace as long as (1) the remaining term on the Reserved Instance is greater than one month, and (2) your payment of the upfront charge for it has been received and processed (for credit card purchases, 30 days after you have paid the upfront fee, and for invoice purchases, after you have paid the applicable invoice) (a **"Marketable EC2 Reserved Instance"**). The characteristics of the Marketable EC2 Reserved Instance (e.g., Instance Type, Platform, Region, Availability Zone, Tenancy, Hypervisor, Reserved Instance Type, Duration, and Hourly Price) will remain as originally designated. The term for the Marketable EC2 Reserved Instance will be the remainder of the original EC2 Reserved Instance term rounded down to the nearest month (for example, an EC2 Reserved Instance with 9 months and 16 days until expiration will be listed and sold as a 9 month Marketable EC2 Reserved Instance). You can be a "Seller" if you are a current AWS customer in good standing, you have a Marketable EC2 Reserved Instance associated with your AWS account, and you complete the registration process through your AWS account. Non-U.S.-based entities may not be Sellers without providing the Form W-8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding) to establish that you are not a U.S. person. You can be a "Buyer" if you are a current AWS customer in good standing. You can resell an EC2 Reserved Instance that you previously purchased through the RI Marketplace. You may not resell an EC2 Reserved Instance that you purchased through a discount program (Reserved Instance Volume Discounts or otherwise) without obtaining our prior approval.

4.6.2. Submitting Marketable EC2 Reserved Instance for Sale. As a Seller, you will set the one-time price for your Marketable EC2 Reserved Instance. The hourly price will be the then-current hourly price for that type of EC2 Reserved Instance, and you will not receive any funds collected from payments associated with the hourly prices. You will pay the then-current fee to us specified on the AWS Site when your Marketable EC2 Reserved Instance is sold. Your Marketable EC2 Reserved Instance will be available for sale after you list it in the RI Marketplace, but it will remain yours and you will be able to use it until it is sold. You may remove a listing of Marketable EC2 Reserved Instance from the RI Marketplace at any time before it has been purchased by a Buyer. We may remove Marketable EC2 Reserved Instance from the RI Marketplace at any time for any reason. Once sold and transferred to a Buyer, a Seller will have no rights to that Marketable EC2 Reserved Instance.

4.6.3. Our Role. As a Seller, you will be the seller of record of your rights to a Marketable EC2 Reserved Instance. Except as expressly set forth in these Service Terms, we are not involved in any underlying transaction between you and any Buyer. We or our affiliates may also participate in the market as a Seller or a Buyer.

Marketable EC2 Reserved Instance through the RI Marketplace. **"Transaction Proceeds"** means the gross sales proceeds received by us from any Transaction. You will ensure that all fees and charges payable by Buyers for Marketable EC2 Reserved Instance are billed and collected through us and you will not offer or establish any alternative means of payment. We may impose transaction limits on some or all Buyers and Sellers relating to the value of any Transaction or disbursement, the cumulative value of all Transactions or disbursements during a period of time, or the number of Transactions that we will process over a period of time. We may withhold for investigation, or refuse to process, any of your Transactions that we suspect is fraudulent, unlawful or otherwise violates the terms of these Service Terms, the Agreement, or our Acceptable Use Policy. For each Transaction, we will not remit Transaction Proceeds to a Seller, and the Marketable EC2 Reserved Instance will be available to the Buyer, until after we have successfully processed payments for that Transaction from the Buyer.

4.6.5. Remittance of Transaction Proceeds to Sellers. At the end of each business day, we will pay to you all due and payable Transaction Proceeds that we have collected as of the date that is 2 business days prior to the date of payment. We will deduct from each payment any applicable fees and charges due to us related to Marketable EC2 Reserved Instances. The applicable fees and charges are posted on the AWS Site and may be changed from time to time. We may withhold, deduct, or setoff any amounts payable by you to us or our affiliates against any Transaction Proceeds. Payments will be made only to an ACH-enabled bank account located in the United States that you register with us. If there is an error in the processing of any Transaction, you authorize us to initiate debit or credit entries to your designated bank account, to correct such error, provided that any such correction is made in accordance with applicable laws and regulations. If we are unable to debit your designated bank account for any reason, you authorize us to resubmit the debit, plus any applicable fees, to any other bank account or payment instrument that you have on file with us or to deduct the debit and applicable fees from future Transaction Proceeds.

4.6.6. Taxes. Sellers are responsible for the calculation, validation and payment of any and all sales, use, excise, import, export, value added, withholding and other taxes and duties assessed, incurred or required to be collected ("**Taxes**") or paid for any reason in connection with any Transaction and with Marketable EC2 Reserved Instance. We are not obliged to determine whether any Taxes apply to any Transaction, and we are not responsible for remitting Taxes to any taxing authority with respect to any Transaction, or for reporting any information (including the payment of Taxes) with respect to any Transaction. Each Seller will indemnify us and our affiliates against any claim or demand for payment of any Taxes imposed in connection with any Transaction, and for any fines, penalties, or similar charges imposed as a result of the Seller's failure to collect, remit or report any Taxes in connection with any Transaction.

4.6.7. Data Collection and Sharing. For each Seller, we will collect the necessary data and tax forms to enable compliance with applicable tax laws. For example, for U.S.-based Sellers, we will collect and retain Seller name and address, and may collect the tax identification number and other data as needed to comply with Form 1099K reporting requirements; for non-U.S.-based Sellers, we will collect and retain a Form W-8BEN tax form (which includes name, address, and a signature) as proof that you are exempt from Form 1099K reporting. For each Buyer, we will collect and retain the Buyer's name and address. Buyers and Sellers will not know the name of the other party to the Transaction until the Transaction is completed. Upon completion of the

legal name on the Buyer's invoice. Buyers and Sellers may not use information about the Transaction or about the other party gained in connection with a Transaction ("**Transaction Information**") for any purpose that is not related to the Transaction. For example, you may not, directly or indirectly: (1) disclose any Transaction Information to any third party, except as necessary for you to perform your tax obligations or other obligations under these Service Terms and only if you ensure that every recipient uses the information only for that purpose and complies with these restrictions; (2) use any Transaction Information for any marketing or promotional purposes whatsoever; (3) use any Transaction Information in any way inconsistent with applicable law; (4) contact a party to influence them to make an alternative sale or purchase; (5) disparage us, our affiliates or any of their or our respective products; or (6) target communications of any kind on the basis of the intended recipient being an RI Marketplace Buyer or Seller.

4.7 You may only use the AWS Management Pack for System Center on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the AWS Management Pack for System Center is governed by the license agreement, located here: AWS Management Pack for System Center License Agreement.

4.8. Dedicated Instances. You may request that certain Amazon EC2 instances run on physically isolated host hardware dedicated to a single customer account (each requested instance, a **"Dedicated Instance"**), using the process set forth on the Amazon EC2 Dedicated Instance detail page on the AWS Site.

4.9. Dedicated Hosts.

4.9.1. You may request that Amazon provide the Amazon EC2 service to you on host hardware physically dedicated to a single customer account (each, a "Dedicated Host"), using the process set forth on the AWS Site.

4.9.2. You may designate Amazon EC2 Dedicated Hosts as subject to the reservation pricing and payment terms ("EC2 Dedicated Host Reservation Pricing") set forth on the Amazon EC2 detail page on the AWS Site (each such host associated with a reservation, an "EC2 Dedicated Host Reservation"). You may associate EC2 Dedicated Host Reservations to Dedicated Hosts by calling APIs or using the EC2 Dedicated Host Reservation console. The EC2 Dedicated Host and associated EC2 Dedicated Host Reservation may only be used in the designated availability zone. We may change EC2 Dedicated Host Reservation Pricing at any time but price changes will not apply to previously designated EC2 Dedicated Host Reservations, except as described in this Section 4.9.2. We may terminate the EC2 Dedicated Host Reservation Pricing program at any time. EC2 Dedicated Host Reservations are nontransferable. EC2 Dedicated Host Reservations are noncancellable and you will owe the EC2 Dedicated Host Reservation Pricing for the duration of the term you selected, even if the Agreement is terminated. Dedicated Hosts associated to an active EC2 Dedicated Host Reservation cannot be unallocated from your account, and you will continue to pay for the Dedicated Host while still associated with the EC2 Dedicated Host Reservation. All amounts paid in connection with the EC2 Dedicated Host Reservations are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual EC2 Dedicated Host type, or terminate the EC2 Dedicated Host Reservation Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated EC2 Dedicated Host Reservation. Upon expiration or termination of the term of an EC2 Dedicated Host

Pricing, EC2 Dedicated Host Reservations are subject to all data transfer and other fees applicable under the Agreement.

4.10. Microsoft BYOL Licensing. Under this option, Amazon EC2 enables you to provision Amazon EC2 instances using your Microsoft Software and Microsoft Licenses (the "BYOL Program"). Unless otherwise specified in your agreement(s) with Microsoft, you can use this benefit only if you comply with the requirements here, and you (a) use Dedicated Instances or Dedicated Hosts; (b) launch from Virtual Machines (VMs) sourced from software binaries provided by you; and (c) run the instances within your designated AWS regions.

You must be eligible to use the BYOL Program for the applicable Microsoft software under your agreement(s) with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. Further, you must have accepted Microsoft's End User License Agreement (Microsoft EULA), and by using the Microsoft Software under the BYOL Program, you agree to the Microsoft EULA.

You agree that you have determined that your use of the BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted.

4.11. As part of using Amazon EC2, you agree that your Amazon EC2 resources may be terminated or replaced due to failure, retirement or other AWS requirement(s). We have no liability whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from the foregoing. THE USE OF AMAZON EC2 DOES NOT GRANT YOU, AND YOU HEREBY WAIVE, ANY RIGHT OF PHYSICAL ACCESS TO, OR PHYSICAL POSSESSION OF, ANY AWS SERVERS, EQUIPMENT, REAL OR PERSONAL PROPERTY, OR OTHER ASSETS.

5. Alexa® Web Services

5.1. You may use Alexa® Web Services to create or enhance applications or websites, to create search websites or search services, to retrieve information about websites, and to research or analyze data about the traffic and structure of the web.

5.2. You may not display data you receive via the Alexa® Services that has been cached for more than 24 hours.

5.3. You may not resell or redistribute the Alexa® Web Services or data you access via the Alexa® Web Services.

5.4. You may use data you receive from the Alexa® Web Services, such as web site traffic data, to enhance your application or website, but may not use it in any application whose primary purpose is to display the same or related data or whose primary purpose is to compete with www.alexa.com.

6.1. The terms in this Section 6 apply only to Amazon FPS and use of Your Content with the web-based payment service provided by Amazon Payments, Inc. (**"Amazon Payments"**) that enables the processing of payment transactions initiated by third parties, and that may include, without limitation, the processing and settlement of credit card transactions, bank transfers, or the administration of prepaid or post-paid balances (the **"Payment Service"**).

6.2. You may:

- access and use Amazon FPS to enable use of the Payment Service by users who have an appropriate Payment Service account (each, an **"Amazon Payments User"**) via Your Content in accordance with any applicable FPS Specifications (as defined below);
- install, copy, and use the software development kit provided by us as part of Amazon FPS, including the related development guides and technical documentation (collectively, the **"FPS SDK"**), and access and use the online testing environment made available by us (the **"FPS Sandbox"**), in each case as necessary to internally develop and test Your Content for use with the Payment Service; and
- create, incorporate, compile, and copy derivative works of the sample computer programming code provided by us for development and testing of Your Content (the **"FPS Sample Code"**) as part of Your Content for distribution in machine readable binary form or object code form to Amazon Payments Users as necessary for them to use the Payment Service. Use of FPS Sample Code is also subject to any additional license terms included with the FPS Sample Code. Such additional terms will control in the event of any inconsistency or conflict with the Agreement.

6.3. The FPS SDK, FPS Sample Code, and FPS Specifications (as defined below) constitute Amazon Properties. Except as expressly authorized by this Section 6, you may not sublicense, loan, sell, assign, lease, rent, transfer, act as a service bureau, distribute or grant rights to any person or entity in Amazon FPS, the FPS SDK, the FPS Sandbox or the Payment Services.

6.4. You and Your Content will comply with any technical and operational specifications and other documentation or policies provided or made available by us or Amazon Payments with respect to Amazon FPS or the Payment Service respectively (the **"FPS Specifications"**). We reserve the right to update or modify the FPS Specifications at any time. Prior to making Your Content generally available for commercial use, you will thoroughly test Your Content to ensure that it operates properly with Amazon FPS, including without limitation that it complies with the FPS Specifications.

6.5. We may review and test Your Content to confirm that it operates properly with Amazon FPS and complies with the FPS Specifications, using review and test processes determined in our sole discretion. You agree to correct any material errors, defects or other non-compliance of which you become aware, including from review and test results provided by us. We may make modifications, updates or upgrades to Amazon FPS, the FPS SDK, or FPS Specifications. In such event, you will test and, if necessary, modify Your Content to ensure that it continues to operate properly with the then-current version of Amazon FPS, the FPS SDK, and FPS Specifications.

to Amazon Payment's policies, procedures, and user agreements, and any breach of the foregoing will constitute a breach of the Agreement. In addition to the limitations described in the Agreement, any use of the Amazon Payments logo and trademark is subject to the trademark usage guidelines issued by Amazon Payments.

6.7. You are responsible for (a) the collection and payment of any and all sales, use, excise, import, export, value added and other taxes and duties assessed, incurred or required to be collected or paid for any reason in connection with any offer or sale of products or services by you, including Your Content, and (b) any payment transaction that is initiated using Your Content that is charged back or reversed (a **"Chargeback"**) to the extent that such Chargeback is attributable to any error, act or omission of you or Your Content and is not otherwise recovered by Amazon Payments from an Amazon Payments User. You will indemnify and reimburse Amazon Payments and its affiliates against any claim or demand for payment of any such taxes or any Chargebacks.

6.8. You represent, warrant, and covenant that you will at all times:

- represent the capabilities and features of the Payment Service consistent with our description of such capabilities and features and avoid false, deceptive, misleading or unethical practices that may be detrimental to us or Amazon Payments, the Payment Service, Amazon Payments Users or other third parties;
- refrain from providing warranties or disclaimers with respect to the Payment Service;
- promptly investigate and report to us all complaints received by you with regard to Amazon FPS and the Payment Service, and make every reasonable effort to maintain and promote good public relations for us in the handling of any such complaints; and
- ensure that the terms of any agreements between you and any Amazon Payments User are consistent with the terms of the Agreement and these Service Terms.

7. Amazon DevPay Service (Amazon DevPay)

7.1. You may use Amazon DevPay to: (a) sell to end users (**"DevPay Customers"**) use of Your Content that you develop and make available with the Services (the **"Bundled Application"**), including machine images that you develop; (b) establish accounts for DevPay Customers that use the Bundled Application (**"DevPay Customer Accounts"**); (c) manage features of DevPay Customer Accounts; and (d) receive payments from DevPay Customers for purchasing Bundled Applications (your "DevPay Transactions").

7.2. You will establish the pricing applicable to DevPay Customers for their use of any Bundled Application. We will only be responsible for collecting those fees that are fully disclosed and properly configured within the DevPay Service. The fees you charge to DevPay Customers for your Bundled Applications through the DevPay Service (as further described in Section 7.6 below) must constitute the full and complete fees you charge DevPay Customers for such Bundled Applications. You may not charge or impose any additional or supplemental fees for Bundled Applications other than those disclosed through the DevPay Service. While you

other than the Bundled Application sold through the DevPay Service.

7.3. You are responsible for designating all terms and conditions applicable to the use of the Bundled Application; provided that, use of the underlying Services are subject to the terms of the Agreement which will control in the event of a conflict. We may require users to register an AWS account (including agreeing to the terms of the Agreement) in order to use Amazon EC2 or other Services associated with the Bundled Application. You may not extend on behalf of us any written or oral warranty or guarantee, or make any representation or claim, with respect to the Services without our prior written consent. Upon termination of the Agreement for any reason, all access by DevPay Customers with respect to your Bundled Applications may be terminated by us.

7.4. Payment Terms.

a. Processing of DevPay Transactions; Collection of DevPay Transaction Proceeds. You hereby appoint us as your payment processing agent for the limited purpose of processing payments, refunds, and adjustments for your DevPay Transactions, We will process all payments refunds, and adjustments for DevPay Transactions and collect the applicable gross sales proceeds received by us from any DevPay Transaction ("DevPay Transaction Proceeds") on your behalf. We do not guarantee payment on behalf of any DevPay Customers. We may withhold for investigation, or refuse to process, any of your DevPay Transactions that we suspect is fraudulent, unlawful or otherwise violates the terms of the Agreement or these Service Terms.

When a DevPay Customer concludes a DevPay Transaction, you authorize us to commit the DevPay Customer's payment less any applicable fees or other amounts we may collect under these terms ("Net Transaction Proceeds") to you. You agree that DevPay Customers satisfy their obligations to you for your DevPay Transactions when we receive the DevPay Transaction Proceeds. We will remit Net Transaction Proceeds to you in accordance with the Agreement and these Service Terms.

b. Remittance of Net Transaction Proceeds to You. Once a month, we will pay to you all previously unpaid Net Transaction Proceeds that we have collected as of the date that is 2 business days prior to the date of payment, except that we may withhold payments to you until you have properly set up your bank account in accordance with instructions you receive from us. We will deduct from each Transaction Proceed any processing fee described on the DevPay detail page on the AWS Site. We may also withhold, deduct, or setoff any amounts payable by you to us or our affiliates against any DevPay Transaction Proceeds. All payments to you will be sent through the Automated Clearing House (ACH) system to your designated U.S. bank account. If there is an error in the processing of any DevPay Transaction, you authorize us to initiate debit or credit entries to your designated bank account, to correct such error, provided that any such correction is made in accordance with applicable laws and regulations. If we are unable to debit your designated bank account for any reason, you authorize us to resubmit the debit, plus any applicable fees, to any other bank account or payment instrument that you have on file with us or to deduct the debit and applicable fees from future DevPay Transaction Proceeds.

c. DevPay Taxes. You are responsible for the calculation, invoicing (if required), validation and payment of any and all sales, use, excise, import, export, value-added, withholding and other taxes and duties assessed,

apply to any DevPay Transaction or your Bundled Applications, and we are not responsible for remitting DevPay Taxes to any taxing authority with respect to any DevPay Transaction or your Bundled Applications, or for reporting any information (including the payment of DevPay Taxes) with respect to any DevPay Transaction or your Bundled Applications. Notwithstanding the foregoing, when we are legally obligated by a valid taxing authority, we will collect DevPay Taxes, and we will provide DevPay Customers with a compliant tax invoice where we are required to do so.

d. If we are unable to collect the DevPay Transaction Proceeds or a prior transaction for those DevPay Transaction Proceeds is reversed, you will not be responsible for paying the fees for the Services used by you and your DevPay Customer ("Service Fees") and AWS will have no obligation to remit or otherwise seek collection of the DevPay Transaction Proceeds, provided that the payment failure is due to:

- AWS's inability to charge a DevPay Customer's credit card for the DevPay Transaction Proceeds, or
- A transaction is reversed as a result of a chargeback because the transaction was not authorized or was otherwise fraudulent.

In addition, in the applicable month, the DevPay Transaction Proceeds charged must exceed the Service Fees. In the event of such a payment failure, we may recover or otherwise set off any DevPay Transaction Proceeds from you that we collected in the month to the extent they do not exceed the Service Fees. In the event that either you or AWS is subsequently able to collect the DevPay Transaction Proceeds, you will pay to AWS the corresponding Service Fees as provided in the Agreement

e. Cancellations and Refunds. You will post your cancellation and refund policy in the Subscription Information, defined below, for your Bundled Applications. At a minimum, this cancellation and refund policy must: (a) allow DevPay Customers who subscribe to your Bundled Applications through a DevPay Transaction to cancel on-going subscriptions for your Bundled Applications through the DevPay detail page on the AWS Site; and (b) comply with these Service Terms. You will accept and process cancellations of, and provide refunds and adjustments for, your Bundled Applications in accordance with the cancellation and refund policy posted at the time of the applicable DevPay Transaction. You will route all DevPay Transaction refund (and adjustment) payments through us. We will credit the applicable account, and you will reimburse us for all amounts so refunded.

7.5. Except as set forth in Section 7.4 above, you are fully liable for all charges incurred for Services under your account identifiers or those assigned to your DevPay Customers for your Bundled Applications. All Services will be charged at the then current price applicable to such Services under the Agreement. Payments will be processed by AWS and are subject to the terms set forth in the Agreement and these Service Terms, including your liability for chargebacks.

7.6. We will host and make available to DevPay Customers a customer interface (**"Customer UI"**) permitting (a) the display to DevPay Customers of certain pricing, terms and conditions and other information you provide to us regarding your Bundled Applications (**"Subscription Information"**) and (b) DevPay Customers to engage in certain functions with respect to your Bundled Applications, such as account establishment, account termination, payment authorization and termination rights. We will define and control the fields and format

7.7. You are responsible for ensuring and shall ensure that all Subscription Information (as you provide it to us and as it is ultimately shown on the Customer UI) is: (a) full, accurate and complete, (b) not misleading; and (c) in compliance, in all respects, with applicable laws. You must promptly update the Subscription Information when and as necessary to ensure that the Subscription Information continues to comply with the foregoing requirements, even if the updates are necessary as a result of changes we make to the data input fields or to the Customer UI.

7.8. You are responsible for providing customer service (if any) to DevPay Customers for your Bundled Applications. We shall have no obligation to provide customer or technical support to any DevPay Customer for Bundled Applications; provided that, we will provide support to DevPay Customers regarding billing and payment questions.

7.9. You will use the communication methods we establish through the DevPay Services for the administration of DevPay Customer Accounts, including, but not limited to, any communications regarding DevPay Customer Account termination or pricing changes.

7.10. You acknowledge and agree that we may take any of the corrective action regarding DevPay Customer Accounts to the extent we deem necessary or appropriate, in our sole discretion, to (a) comply with law, (b) enforce or apply the Agreement, and these Service Terms, or other agreements or policies applicable to the Services or DevPay Service, or (3) protect the rights, property or safety of our business, a DevPay Customer, or any third party. Corrective action may include (i) suspending, canceling or closing of DevPay Customer Accounts; (ii) re-establishment of DevPay Customer Accounts; and (iii) waiving or refunding of fees on DevPay Customer Accounts. We shall have no liability to you for taking any such actions. You shall promptly comply with any actions we take or may require of you regarding DevPay Customer Accounts. These actions may include, without limitation, reimbursing us for DevPay Customer refunds we issue, discontinuing provision of services on DevPay Customer Accounts we cancel, and re-establishment of services on DevPay Customer Accounts we re-establish. Should you ask us to close a DevPay Customer Account by using a method we have provided for that purpose, we will endeavor to close the DevPay Customer Account reasonably promptly, but we shall have no liability to you for the speed with which we do so or for our failure to do so. You shall indemnify and hold us and our employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys fees), arising out of or in connection with any claim based on or related to any actions we may take with respect to any DevPay Customer Account at your direction, including, without limitation, any closure of a DevPay Customer Account.

7.11. You acknowledge and agree that: (a) you have no expectation and have received no assurances that your business relationship with us will continue beyond the Term (or its earlier termination), that any investment by you in the promotion of any Bundled Application will be recovered or recouped, or that you will obtain any anticipated amount of profits; and (b) you will not have or acquire by virtue of the DevPay Services or otherwise any vested, proprietary or other right in the promotion of any Services or in any related goodwill created by your efforts.

8.1. If during the previous six (6) months you have incurred no fees for Amazon SimpleDB and have registered no usage of Your Content stored in Amazon SimpleDB, we may delete, without liability of any kind, Your Content that is stored in Simple DB upon thirty (30) days prior notice to you.

9. Amazon Fulfillment Web Service (Amazon FWS)

9.1. You may only access and use Amazon FWS to query, access, transmit and receive product and shipping information related to your use of the Fulfillment by Amazon service (**"FBA Service"**) sold and provided by Amazon Services LLC (**"Amazon Services"**) in accordance with any applicable FBA Specifications (as defined below).

9.2. To use Amazon FWS, you must have an Amazon seller account (your **"Seller Account"**) that is in good standing and be registered to use the FBA Service. Your use of the FBA Service and your Seller Account is solely subject to Amazon Services' policies, procedures, the Amazon Business Services Agreement or other applicable user agreements. Amazon FWS is only a technical interface that enables you to access and process certain information related to your Seller Account. AWS will have no liability to you or any third party related to your Seller Account.

9.3. You may use Amazon FWS only to administer product and shipping information associated with your Seller Account. When registering for Amazon FWS, you must use the same username and password which is associated with your Seller Account. You may not develop or use an application to access Amazon FWS that collects, processes or stores the account identifiers or other security credentials (including usernames and passwords) of any third party associated with AWS or any of its affiliates.

9.4. You and Your Content will comply with any technical and operational specifications, security protocols and other documentation or policies provided or made available by us with respect to Amazon FWS (the **"FBA Specifications"**). We reserve the right to update or modify the FBA Specifications at any time. Prior to making Your Content available for commercial use, you will thoroughly test Your Content to ensure that it operates properly with Amazon FWS, including, without limitation, that it complies with the FBA Specifications.

10. Amazon Elastic MapReduce

10.1. We may collect certain information about computing jobs you run using Amazon Elastic MapReduce, including CPU utilization, memory usage, IO performance, and error and information messages.

10.2. You are responsible for all fees incurred from your use of Amazon Elastic MapReduce regardless of the results obtained, the quality of the resulting data, or whether a computing job runs successfully. Use of Amazon Elastic MapReduce requires use of Amazon EC2 and Amazon S3, and certain features require use of Amazon SimpleDB. You are responsible for the separate fees you accrue for Amazon EC2, Amazon S3, and Amazon SimpleDB.

Services, or any component of the Services. We are not responsible for any data loss or data corruption that occurs as part of your computing jobs.

11. Amazon CloudWatch and Auto Scaling

11.1. Automatic scaling services, including AWS Auto Scaling, Amazon EC2 Auto Scaling, and Application Auto Scaling (collectively, "Auto Scaling Services") require use of both Amazon CloudWatch and other supported Services.

11.2. In connection with Auto Scaling Services, we may launch/add additional supported Services/capacity or terminate/remove those Services/capacity based on conditions you set. You are responsible for the separate fees you accrue for such Services. You are responsible for all fees incurred from your use of Amazon CloudWatch and Auto Scaling Services regardless of the results obtained or the quality or timeliness of the results. Charges for Amazon CloudWatch will accrue as soon as you use begin using Amazon CloudWatch or Auto Scaling Services.

11.3. Amazon CloudWatch collects and stores certain information for the Services you are monitoring, including CPU utilization, data transfer, and disk usage and activity. Amazon CloudWatch metric data is made available to you for the applicable retention period listed on the AWS Site; we may delete CloudWatch metric data, without liability of any kind, at any time after the applicable retention period.

12. Elastic Load Balancing

12.1. You may only use Elastic Load Balancing to provide load balancing functionality in connection with the Services. You must have instances running in all Availability Zones across which you want to balance loads with Elastic Load Balancing.

12.2. Use of Elastic Load Balancing requires use of other Services. You are responsible for the separate fees you accrue for the Services. You are responsible for all fees incurred from your use of Elastic Load Balancing regardless of the results obtained or the quality or timeliness of the results. Charges for Elastic Load Balancing will accrue as soon as you use begin using Elastic Load Balancing functionality.

13. AWS Import/Export Disk, AWS Snowball, and AWS Snowmobile

13.1. As part of AWS Import/Export Disk, you may send physical storage media (the "Media") to us that we will use to either (a) transfer data contained on the Media into supported AWS Services as Your Content, or (b) transfer certain of Your Content to the Media (such data contained on Media either before or after transfer, "Data") and provide the Media to you. You will not deliver to us, and we may refuse to accept, any damaged, defective or unreadable Media or any Media otherwise not shipped in accordance with the Agreement (collectively, "Unsuitable Media"). We may return or dispose of any Unsuitable Media, or erase Data on such Unsuitable Media, and you will reimburse us for any expenses we incur in connection with any Unsuitable Media. If you request and we return Unsuitable Media to you, you agree that we will select the shipping carrier

with AWS Import/Export generally. For avoidance of doubt "Media" includes "Unsuitable Media".

13.2. As part of AWS Snowball, we will ship you an agreed upon number of "Snowball" hardware appliances (each an "Appliance") and provide you with access to the AWS Snowball Client (together with the software contained on the Appliance, and any updates or upgrades to the foregoing, the "Snowball Software"). You agree that you will not allow any Appliance to leave the United States state or non-U.S. country to which the Appliance is shipped until you provide it (in the same U.S. state or non-U.S. country) to a carrier for redelivery to us. After you receive an Appliance, you may: (a) transfer data onto the Appliance for upload by us into a supported AWS Service as Your Content after you return the Appliance, (b) transfer data you requested we copy to the Appliance onto your own systems, and provide the Appliance to the carrier for return to us (such data in (a) or (b) contained on Appliances before, during, or after transfer, also "Data"), or (c) if using a "Snowball Edge" Appliance as described on the AWS Site, transfer Data onto the Appliance and use the Appliance for certain computing workloads as described in the Documentation. We may require that Appliances be returned to us at any time for any reason, including for repair and replacement, and you will promptly return such Appliances to us. Appliances collect and provide us with metrics regarding the use of Appliances, including without limitation boot times, size of transferred files, duration of transfers, and errors or timeouts. These metrics may be associated with your account ID and we may use these metrics to provide, maintain, and improve the quality and feature set of the Service Offerings.

13.3. As part of AWS Snowmobile, we will transport a containerized data center and networking equipment (collectively, "Snowmobile"), and, in certain cases, auxiliary power and chilling units, to a designated transfer location (the "Transfer Site"). The Snowmobile, power generator, chiller unit, related vehicles, and all software provided in connection with the foregoing are collectively "Snowmobile Materials." You will cooperate with us to meet all requirements for deploying Snowmobile Materials, including surveying, securing and maintaining the Transfer Site, obtaining all necessary licenses and permits for operation of the Snowmobile Materials at the Transfer Site, and allowing access for us and our affiliates' employees, subcontractors, and agents (collectively, "Snowmobile Personnel") to setup, maintain, inspect, repair, operate and remove Snowmobile Materials. After Snowmobile Materials are deployed, you may transfer data onto the Snowmobile (such data contained on the Snowmobile before, during, or after transfer, also "Data"). Once the transfer is complete, authorized Snowmobile Personnel will transport the Snowmobile to the selected AWS region for upload of Data into a supported AWS Service as Your Content.

13.4. You will comply with all specifications and documentation for AWS Import/Export as provided and updated by us from time to time, including shipping and encryption requirements, the AWS Import/Export Disk Pack and Ship Check List, the AWS Snowball User Guide, and any documentation on the AWS Site or an Appliance.

13.5. You will be solely responsible for all shipping and handling costs (which may include costs of freight and transit insurance) for shipping Media and Appliances to or from us. For AWS Import/Export Disk, we may pay some reasonable return shipping charges as described on the AWS Import/Export Disk section of the AWS Site. You are responsible for payment of all customs, duties, taxes and other charges in connection with Media and Appliances being shipped to or from us. Use of AWS Import/Export may require or allow use of supported

13.6. For AWS Import/Export Disk, you will bear the entire risk of loss of, or damage to, any Media while in transit and you are solely responsible for obtaining insurance at your expense. For AWS Snowball, you are responsible for any damage to, an Appliance after it has been delivered by the carrier to your address until the carrier accepts the Appliance for delivery back to us, and we may charge you the cost of fixing such damage. For Appliances that are not Snowball Edge Appliances, we may charge you $7,500 USD if the Appliance is lost or irreparably damaged after it has been provided to you until the carrier accepts the Appliance for delivery back to us, or if you do not provide the Appliance to the carrier for return to us within 90 days of the date it was delivered to you. For Snowball Edge Appliances, we may charge you $15,000 USD if the Appliance is lost or irreparably damaged after it has been provided to you until the carrier accepts the Appliance for delivery back to us, or if you do not provide the Appliance to the carrier for return to us at our request. For avoidance of doubt, amounts charged under this Section do not limit your liability under this Agreement. For AWS Snowmobile, you are responsible for any damage to, or loss of, Snowmobile Materials once they arrive at the Transfer Site until the Snowmobile Materials depart the Transfer Site under the supervision of authorized Snowmobile Personnel. You may not allow Snowmobile Materials to leave the Transfer Site other than under the supervision of authorized Snowmobile Personnel.

13.7. You will retain title to any Media and Data we receive from you and store on an AWS Service (or provide to you upon your request) as part of AWS Import/Export. You supply us with Media and Data, and you use Media, Appliances, Snowball Software, and Snowmobile Materials entirely at your own risk. You should back-up Data prior to transfer onto an Appliance, Snowmobile or Media and prior to delivery to us, and you should not delete any of Your Content on an AWS Service before transferring such content from an Appliance, Snowmobile or Media onto your own systems. Your Data should not include live or production data or any other data that you are not prepared to lose. We are not responsible for and will not be held liable for any delay, damage or loss incurred in connection with AWS Import/Export, including without limitation loss, damage, destruction or misuse of any Data or any systems or equipment used in connection with AWS Import/Export. Our confirmed receipt of delivery or notification of shipment or transport does not: (a) indicate or imply that any Media, Appliance, Snowmobile Materials, or Data has been or will be delivered or was received free of loss, damage or destruction, or that any loss or damage to, or any destruction of, any Media, Appliance, Snowmobile Materials, or Data later discovered is not your responsibility; (b) indicate or imply that we actually received the number of units of Media or Appliances specified by you for such shipment; or (c) waive, limit or reduce any of our rights under the Agreement. We reserve the right to impose, and change, from time to time, limitations on the delivery of your Media or Data, and you will comply with any of these restrictions or limitations.

13.8. You represent that you have all necessary rights to (a) provide the Media and/or Data (whether contained on an Appliance, Media or Snowmobile) to us for upload into supported AWS Services, (b) receive Appliances and/or Snowmobiles and use them as permitted by us, (c) transfer Data to the Media, Appliance or Snowmobile, and (d) authorize our transfer of any Data specified by you to the Media, Appliance or Snowmobile and to you. Without limiting the foregoing, if Data includes personal information, personally identifiable information, personal data, any information about a person or individual, or any other data covered by applicable law or regulation, you represent that you have obtained all necessary rights to transfer

of such Data. We may reproduce Data as necessary to transfer it between Media, Appliances or Snowmobiles and supported AWS Services.

13.9. IN ADDITION TO THE DISCLAIMERS IN THE AGREEMENT, WE HEREBY DISCLAIM ANY DUTIES OF A BAILEE OR WAREHOUSEMAN, AND YOU HEREBY WAIVE ALL RIGHTS AND REMEDIES OF A BAILOR (WHETHER ARISING UNDER COMMON LAW OR STATUTE), RELATED TO OR ARISING OUT OF ANY POSSESSION, STORAGE OR SHIPMENT OF MEDIA OR DATA BY US OR OUR AFFILIATES OR ANY OF OUR OR THEIR CONTRACTORS OR AGENTS. YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA AND YOUR USE OF MEDIA, APPLIANCES AND SNOWMOBILE MATERIALS, INCLUDING ENCRYPTING SENSITIVE DATA AND NOT ALLOWING UNAUTHORIZED ACCESS TO ANY MEDIA, APPLIANCE OR SNOWMOBILE.

13.10. In addition to your indemnification obligations under the Agreement, you agree to indemnify, defend and hold us, our affiliates and licensors, each of our and their business partners (including third party sellers on websites operated by or on behalf of us) and each of our and their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys' fees), arising out of or in connection with any claim arising out of the Media, Data, and your use of Appliances, Snowball Software or Snowmobile Materials, including (a) any personal injury, death or property damage (tangible or intangible) related to the foregoing; (b) any sales, goods and services, use, excise, import, export, property, value added or other taxes or duties assessed or imposed on us or our affiliates in connection with or as a result of the storage, shipping or other actions taken by you or us with respect to your use of AWS Import/Export; or (c) any legal or regulatory violation arising under the laws or regulations of any country (including without limitation privacy regulations) related to your use of AWS Import/Export.

13.11. Once AWS Import/Export services are complete, we will return the Media to you or destroy Unsuitable Media, delete Data from the Appliance, or delete Data from the Snowmobile, as applicable. We may return Media to you for any reason, including upon termination of the Agreement or the AWS Import/Export Service. Returned Media will be sent to your designated shipping address. Media shipped to us for import into or export from supported AWS Services in the EU (Ireland) Region must originate from and be returned to an address within the European Union or the European Economic Area. If we are unable to return Media to you due to any issue with your address or Media, we will attempt to notify you, and you will have thirty (30) calendar days from the date we provide notification to resolve the issue. If the issue is not resolved, the Media will be deemed Unsuitable Media subject to disposal and we may erase Data and dispose of Media in any manner and we have no obligation to reimburse or compensate you in connection with such erasure or disposal.

13.12. Notwithstanding anything to the contrary in the Agreement, you may give agents and subcontractors of your choosing access to the private key associated with your AWS account solely for the purpose of (a) preparing Data for import, export or processing using AWS Import/Export or (b) confirming the integrity of Data imported, exported or processed using AWS Import/Export. You remain fully responsible for and indemnify us for all activities undertaken by such third parties under your account. Other than as specifically

13.13. The Appliances, Snowmobile Materials ,Snowball Software and all other proprietary information, know-how, programming, software, trademarks, trade secrets, plan drawings, requirements, specifications, designs, and patterns furnished or created by us or our agents or contractors and all property rights embodied therein are and will remain our sole property at all times. Except as explicitly stated, at no point do we sell, rent, lease or transfer any ownership or other rights to the Appliance or Snowmobile Materials to you. You may not use the Appliance or Snowmobile Materials in any manner not expressly permitted herein. Without limiting the foregoing, you will not (or attempt to), and will not permit or authorize third parties to (or attempt to), (a) reverse engineer, disassemble, or decompile the Appliance or the Snowball Software or Snowmobile Materials or apply any other process or procedure to derive the source code of any Appliance, Snowball Software or Snowmobile Materials; (b) scan, x-ray, open, modify, alter, disassemble or otherwise attempt to view the inside of or tamper with the Appliance or Snowmobile Materials; (c) access, move or relocate the Snowmobile Materials in any way; or (d) circumvent or disable any features or measures in the Appliance, Snowball Software or Snowmobile Materials. Snowball Software contained on Appliances is a "Service Offering" and your use of such Snowball Software is governed by the applicable terms of the Agreement. Your use of the AWS Snowball Client and any downloadable Snowball Software is governed by the licenses included with such Snowball Software.

13.14. We will be responsible for monitoring, maintaining, repairing, and updating components of the AWS Snowball service, including Snowball Software and Appliances. You will return all Appliances to us regardless of the external condition of the Appliance and even if you believe the Appliance may be damaged or non-functional. Although the used Appliance is not waste electrical and electronic equipment, and you will not be the final user of the Appliance, for the avoidance of doubt you understand that the Appliance is not to be disposed of as waste electrical and electronic equipment, including as unsorted municipal waste or in any other waste collection process, that your return of the Appliance to us according to the terms of the Agreement will contribute to extension of the useful life of the Appliance and its responsible handling and recycling by us when it reaches its end of life, and that the disposal or improper handling of the Appliance, as with other electrical and electronic equipment, could have potentially adverse effects on the environment and human health as a result of the presence of hazardous substances in such equipment. For avoidance of doubt, the terms of this Section also apply to internal batteries included within Appliances. You are not permitted to access, move or relocate the internal batteries of Appliances. The Appliance is marked with a crossed-out wheelie bin symbol to reflect these requirements and in compliance with waste-related regulatory requirements in certain jurisdictions.

13.15. For AWS Import/Export Disk, we will not act as the importer of record for your shipments of Media or Data. If we are importing or exporting your shipments of Media or Data into the Asia Pacific (Singapore) Region, you will not act as the importer of record and you represent and warrant that: (a) You are not a resident of Singapore; (b) You have a business establishment or fixed establishment outside of Singapore and not in Singapore; (c) You are domiciled outside Singapore if you have no business or fixed establishment in any country; and (d) You are not registered or required to be registered for GST in Singapore.

to make any of the above representations and warranties.

If you are not acting as the importer of record on your shipment of Media or Data to the Asia Pacific (Singapore) Region, then the Media or Data must (i) be returned to a location outside of Singapore, (ii) be exported on an FCA basis; and (iii) you must be importer of record in the country that the Media or Data is returned to.

13.16. You are responsible for complying with all applicable data protection, import, re-import, export, and re-export control laws, including any applicable license requirements, and country-specific sanctions programs. Without limiting the foregoing, you are solely responsible for compliance related to the manner in which you use Appliances, Media, Snowball Software or Snowmobile Materials, including your transfer, upload, and download of your data, goods, software, or technology and the provision of your data, goods, software, or technology to End Users. You are responsible for serving as the exporter and importer of record (as applicable) for your Media, data, goods, software, or technology, and you accept that AWS will not participate in the export or import procedure. If you are using Appliances, Media, Snowball Software, or Snowmobile Materials for dual use items in the European Union, you represent that you, or the legal entity you represent, are "established" in the European Union; or, if you are not "established" in the European Union, that you will not upload, request that we download, or export such dual-use items outside the European Union. If you are using Appliances, Media, Snowball Software or Snowmobile Materials in the European Union for military items, you represent that you, or the legal entity you represent, are permitted by the Member State of your incorporation to upload, request that we download or export any such military items from that Member State, and it is a condition of this Agreement and your use of AWS Import/Export that you are so permitted.

13.17. We may provide you with custom air filters for use with Appliances ("Filters"). Filters are provided "as is" and we make no representation or warranty regarding Filters. Except to the extent prohibited by law, we expressly disclaim all warranties of any kind related to Filters, including any implied warranties of merchantability, quality, or fitness for a particular purpose. You use Filters entirely at your own risk. We are not responsible and will not be liable for any loss, damage, destruction or misuse of any systems or equipment you use in connection with Filters, including without limitation Appliances.

14. Amazon Virtual Private Cloud (Amazon VPC)

14.1. You may only use Amazon VPC to connect your computing resources to certain AWS computing resources via a Virtual Private Network (VPN) connection.

14.2. Use of Amazon VPC requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with Amazon VPC. When you transfer data between AWS computing resources running inside Amazon VPC and AWS computing resources running outside Amazon VPC, you will be charged VPN data transfer rates in addition to any applicable Internet data transfer changes. VPN connection charges accrue during any time your VPN connection is in the "available" state.

connect to Amazon VPC.

15. AWS Multi-Factor Authentication (AWS MFA)

15.1. You may only use AWS MFA in connection with accessing your AWS account.

15.2. Your use of AWS MFA requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with AWS MFA.

15.3. You are solely responsible for the procurement and for the configuration, operation, performance and security of any hardware or non-AWS software that you use in connection with AWS MFA, including any compatible authentication devices.

16. Amazon Relational Database Service (Amazon RDS)

16.1. You may only use Amazon RDS to store, query, retrieve and serve data and other content owned, licensed or lawfully obtained by you. You acknowledge that neither we nor our licensors are responsible in any manner, and you are solely responsible, for the proper configuration of database security groups and other security settings associated with Amazon RDS.

16.2. You may store snapshots of Your Amazon RDS Content for later use in Amazon RDS but snapshots cannot be downloaded outside the Services.

16.3. We may terminate your Amazon RDS database instance if you attempt to access or tamper with any software we pre-load on the database instance, including the operating system software running on the database instance.

16.4. You are responsible for configuring your backup retention period to give yourself enough time to recover data from your backups in the event of a hardware or file system failure.

16.5. Reserved DB Instance Pricing. You may designate Amazon RDS database instances as subject to the reserved pricing and payment terms ("Reserved DB Instance Pricing") set forth on the Amazon RDS detail page on the AWS Site (each designated instance, a "Reserved DB Instance"). You may designate database instances as Reserved DB Instance by calling to the Purchasing API or selecting the Reserved DB Instance option in the AWS console. When you designate a database instance as a Reserved DB Instance, you must designate a region, instance type and quantity for the applicable Reserved DB Instances. The Reserved DB Instances may only be used in the designated region. We may change Reserved DB Instance Pricing at any time but price changes will not apply to previously designated Reserved DB Instances. We may terminate the Reserved DB Instance Pricing program at any time. Reserved DB Instances are noncancellable, and you will owe the Reserved DB Instance Pricing for the duration of the term you selected, even if the Agreement is terminated. Reserved DB Instances are nontransferable and all amounts paid in connection with the Reserved DB Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual

Upon expiration or termination of the term of a Reserved DB Instance, the Reserved DB Instance Pricing will expire and standard on-demand usage prices will apply to the database instance. In addition to being subject to Reserved DB Instance Pricing, Reserved DB Instances are subject to all data transfer and other fees applicable under the Agreement.

16.6. Using Oracle Software.

16.6.1. "License Included"**.** As part of the Services, you may be allowed to use certain software (including related documentation) described on the AWS Site developed and owned by Oracle America, Inc. or its affiliates (**"Oracle"**) and Oracle's licensors (collectively, the **"Oracle Software"**). If you choose to use the Oracle Software and do not already have a license from Oracle for that Oracle Software, Oracle and its licensors require that you agree to these additional terms and conditions:

- Oracle or its licensors retains all ownership and intellectual property rights in the Oracle Software, and title to the Oracle Software does not transfer to you or any third party by virtue of this Agreement.
- The Oracle Software is subject to a restricted license and may only be used in connection with the Service Offerings, and only by the individual or legal entity that entered into the Agreement.
- You may only use the Oracle Software for your internal business operations and in accordance with the Agreement. You may permit agents or contractors (including outsourcers) to use the Oracle Software on your behalf for the purposes set forth in, and subject to, the Agreement, provided you are responsible for the agent's, contractor's and outsourcer's compliance with the Agreement in connection with such use.
- You may not:
    - assign, grant, or transfer the Oracle Software or any interest in the Oracle Software to another individual or entity, and if you purport to grant a security interest in the Oracle Software, the secured party will have no right to use or transfer the Oracle Software;
    - use the Oracle Software for rental, timesharing, subscription services, hosting, or outsourcing;
    - remove or modify any notice of Oracle's or its licensors' proprietary rights;
    - make the Oracle Software available in any manner to any third party for use in the third party's business operations;
    - duplicate, reverse engineer (unless required by law for interoperability), disassemble or decompile the Oracle Software (including by reviewing data structures or similar materials produced by the Oracle Software); or
    - publish any results of benchmark tests run on the Oracle Software.
- Third party technology that may be appropriate or necessary for use with some Oracle Software is specified in the related documentation, and that third party technology is licensed to you only for use with the Service Offerings and under the terms of the third party license agreement specified in the documentation, not this Agreement.

arising from your use of the Oracle Software.

- Notwithstanding anything to the contrary elsewhere in the Agreement, Oracle is an intended third party beneficiary of the Agreement, but solely with respect to this Section 16.6.1 of these Service Terms.
- The Uniform Computer Information Transactions Act does not apply to your use of the Oracle Software.
- Upon any termination of the Agreement, you must discontinue use of the Oracle Software and any related documentation.

16.6.2. "Bring-Your-Own-License" (BYOL). Under the BYOL option, Amazon RDS enable you to provision Oracle Software to Amazon EC2 instances and use the management capabilities of Amazon RDS for the Oracle Software. You can use the Oracle Software with Amazon RDS if you meet the following conditions:

- You must have a valid license with "Software Update License & Support" for the Oracle Software you wish to run. The terms of your existing license and support agreement(s) with Oracle continue to apply to your use of the Oracle Software; and
- You must follow Oracle's current policies for licensing Oracle Database software in the cloud computing environment. The database instances using the Oracle Software with Amazon RDS reside in the Amazon EC2 environment.

16.7. Using Microsoft Software.

16.7.1. "License Included." In conjunction with the Services, you may be allowed to use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the **"Microsoft Software"**). If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

- The Microsoft Software is neither sold nor distributed to you and you may use it solely in conjunction with the Services.
- You may not transfer or use the Microsoft Software outside the Services.
- You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Software.
- You may not reverse engineer, decompile or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.
- Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.
- You are not granted any right to use the Microsoft Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable

Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.

- SQL Server Web Edition may be used only to support public and Internet accessible Web pages, Web sites, Web applications or Web services. It may not be used to support line of business applications (e.g., Customer Relationship Management, Enterprise Resource Management and other similar applications).

16.7.2. Microsoft is an intended third-party beneficiary of this Section 16.7, with the right to enforce its provisions.

17. Amazon Simple Notification Service (Amazon SNS)

17.1. Amazon SNS from the Asia Pacific (Tokyo) Region is sold and provided by AMCS LLC and not AWS, but is otherwise subject to the terms of the Agreement.

17.2. You may only use Amazon SNS to send notifications to parties who have agreed to receive notifications from you.

17.3. We may throttle or restrict notifications if we determine, in our sole discretion, that your activity may be in violation of the AWS Acceptable Use Policy or the Agreement.

17.4. Your notifications sent through Amazon SNS may be blocked, delayed or prevented from being delivered by destination servers and other reasons outside of our control and there is no warranty that the service or content will be uninterrupted, secure or error free or that notifications will reach their intended destination during any stated time-frame. In addition, you acknowledge that we may not be able to provide the service if a wireless carrier delivering Amazon SNS notifications by short messaging service (SMS) terminates or suspends their service. Your payment obligations may continue regardless of whether delivery of your notifications are prevented, delayed or blocked.

17.5. You may not use Amazon SNS to send SMS messages that include Premium Content (as defined in the Mobile Marketing Association Guidelines). You may not charge recipients for receiving Amazon SNS notifications by SMS unless you have obtained the recipient's express consent. You must advise recipients receiving Amazon SNS notification by SMS that wireless carriers may charge the recipient to receive Amazon SNS notifications by SMS. You must obtain our prior written consent before using Amazon SNS to send SMS messages for:

- financial transactions or payment services (e.g., mobile banking, bill presentment, bill payment, money transfer, peer-to-peer payment or lending credit, debit or stored value payment services);
- charitable programs (e.g., soliciting donations for a non-profit organization);
- sweepstakes or contests;

recipient's wireless device).

17.6. Any third party push notification platform that you use in connection with Amazon SNS is Third Party Content under the Agreement, and features of Amazon SNS that depend on such platforms may not be secure, uninterrupted or error-free. Your use of such push notification platform is subject to the platform's terms and conditions, and you are solely responsible for complying with those terms and conditions. We may change, discontinue or deprecate support for a push notification platform for any reason at any time.

17.7. You and any of your applications that use Amazon SNS must comply with all laws, rules, and regulations applicable in jurisdictions in which your applications are used.

17.8. Through your use of Amazon SNS you will not:

- Transmit any material that contains viruses, Trojan horses, worms or any other malicious, harmful, or deleterious programs.
- Offer or purport to offer any Emergency Services. "Emergency Services" means services that allow a user to connect with emergency services personnel or public safety answering points such as 911 or E911 services.
- Materially violate or facilitate the material violation of any local or foreign law, rule, regulation or order, including laws regarding the transmission of data or software
- Transmit material that is sexually explicit, relates to "adult services", or contains sensitive financial or identifying information (such as social security numbers)
- Resell, sublicense or timeshare the Services or use them on behalf of anonymous or other third parties.
- Use the Services in hazardous environments (such as operation of nuclear facilities, aircraft navigation, or any other use that may result in foreseeable risk of injury, death, or destruction of property).

18. Consolidated Billing

Consolidated Billing has been incorporated into AWS Organizations (See Section 63).

19. AWS Identity and Access Management (IAM)

19.1. You may use IAM to create additional sets of security credentials (the **"User Credentials"**) under your AWS account, the format of which may include a username and password, roles, policies, permissions, access keys, and/or a security token. The User Credentials are subject to change: (a) by you through the IAM APIs, or (b) if we determine in our reasonable discretion that a change is necessary. We will promptly notify you of any change we make to the User Credentials.

19.2. You will ensure that all use of the Services under the User Credentials complies with the terms and conditions of the customer agreement between you and us that governs your use of the Services.

security of the User Credentials (other than any key that we expressly permit you to use publicly). You are solely responsible, and we have no liability, for any activities that occur under the User Credentials, regardless of whether such activities are undertaken by you, your employees, agents, subcontractors or customers, or any other third party. You are responsible for the creation, distribution, and security (including enabling of access) of all User Credentials created under your AWS account, including credentials that you have used IAM to create or disclose to other parties.

19.4. Except as otherwise provided by AWS, you may only use User Credentials for your internal use and may not expose your User Credentials publicly. You may not sell, transfer or sublicense or authorize the creation of User Credentials (other than public use of any key that we expressly permit you to use publicly) to any other party; provided that, you may disclose or cause to be disclosed User Credentials to your agents or subcontractors that are performing services for you, solely to allow the agents or subcontractors to use the Services on your behalf in accordance with the agreement between you and us that governs your use of the Services.

19.5. Any third party identity provider that you use in connection with the Service Offerings is Third Party Content under the Agreement and may be provided directly to you by a third party under separate terms and conditions. You are solely responsible for complying with those terms and conditions. We may change, discontinue or deprecate support for an identity provider for any reason, including if the continued use of the identity service (a) poses a security or intellectual property issue, (b) is economically or technically burdensome, or (c) must be terminated to comply with the law or requests of governmental entities.

20. Amazon Route 53

20.1. You may use Amazon Route 53 to answer Domain Name System (DNS) queries for your applications.

20.2. You will not create a hosted zone for a domain that you do not own or have authority over.

20.3. All DNS records (other than Private DNS records) used in connection with Amazon Route 53 will be publicly available and AWS will have no liability for disclosure of those DNS records.

20.4 Domain name registration services are provided under our Domain Name Registration Agreement.

21. AWS Elastic Beanstalk

21.1. The URL used in connection with an AWS Elastic Beanstalk environment will have the formulation [myapp].elasticbeanstalk.com. You will select the “myapp” portion of the URL and will not:

- include any trademark of Amazon or its affiliates, or a variant or misspelling of a trademark of Amazon or its affiliates – for example, "endlessboots", "amaozn", "smallpartsstore", "amazonauctions", "kindlemagazines", or "kindlewirelessreader" would be unsuitable; or

AWS may reject any URL that fails to comply with this Section. Further, AWS may modify any URL in order to make it compliant with this Section. In addition, AWS may treat any URL that fails to comply with this Section as Prohibited Content.

21.2. The [myapp] portion of the URL is reserved for you only during the time your application environment is running. If you stop running your application environment at any time, for any reason, the [myapp] portion of the URL you were using to run the application environment will no longer be available to you, and will be returned to a pool from which it may be used by another AWS customer.

21.3. AWS may make available reference or sample applications for you to use in connection with AWS Elastic Beanstalk (**"Elastic Beanstalk Sample Apps"**). Elastic Beanstalk Sample Apps are provided "as is" and you will be charged the same fees for running Elastic Beanstalk Sample Apps as you would be charged for running your own application.

21.4. AWS Elastic Beanstalk is offered at no additional charge, but requires the use of other AWS services. You are responsible for all fees incurred for AWS services used in connection with AWS Elastic Beanstalk.

22. Amazon Simple Email Service (SES)

22.1. We take steps to increase the security and reliability of email you send, attempt to send, or receive using SES (**"SES Email"**). Like many email service providers, when you send, attempt to send, or receive an email, we (or our third-party providers) may store and scan your SES Email and Your Content included in SES Email. This helps us protect you and SES by preventing and blocking "spam" e-mails, viruses and spyware, and other harmful or unwanted items from being sent and received over SES.

22.2. Your use of SES and all SES Email must comply with the AWS Acceptable Use Policy and the Agreement. We may throttle, suspend or terminate your access to SES, or block or decline to send and/or receive any SES Email, if we determine in our sole discretion that

- our scan of SES Email or Your Content included in SES Email reveals abusive or low quality email (such as "spam"),
- SES Email bounces back to us or we receive abuse complaints (including complaints from third parties) in connection with your SES Email,
- the source or ReturnPath email address you have provided us for "address bounces" or complaints is not successfully receiving email, or
- your use of SES Email does not comply with the AWS Acceptable Use Policy or the Agreement, or
- your SES Emails or Your Content include an attachment in a format that we do not support.

22.3. Your SES Emails may be blocked, delayed or prevented from being delivered by destination email servers and other reasons outside of our control. Your payment obligations continue regardless of whether delivery of your emails is prevented, delayed or blocked.

in connection with an open mail relay, including, without limitation, an open mail relay in the form of an SMTP server, unrestricted web form, or otherwise.

22.5. Your SES Emails may be blocked, delayed or prevented from being received due to your configuration of the Service. You are solely responsible for the proper configuration of the Service to ensure the receipt of emails.

23. AWS CloudFormation

23.1. You may use AWS CloudFormation to create a collection of AWS resources and provision them.

23.2. AWS may make sample templates available for you to use in connection with AWS CloudFormation. All sample templates are offered "as is" and you are solely responsible for your use of the sample templates.

23.3. Any templates you use in connection with AWS CloudFormation must comply with the Agreement and the AWS Acceptable Use Policy and you are solely responsible for your use of any templates.

23.4. AWS CloudFormation is offered at no additional charge, but requires the use of other AWS services. You are responsible for all fees incurred for AWS services used in connection with AWS CloudFormation.

24. AWS Direct Connect

24.1. You may use AWS Direct Connect to establish a dedicated network connection between your network and your AWS resources by using connection types and locations supported by AWS. When you establish a dedicated connection, your network traffic that would have otherwise been routed over the Internet may be routed through your dedicated network connection, including your network traffic sent to or from (i) services offered by other affiliates of Amazon.com, Inc. or (ii) the AWS resources of other AWS customers.

24.2. The hardware and equipment you use with AWS Direct Connect must comply with the Documentation provided by AWS. You are responsible for protecting your AWS Direct Connect connections, including using physical security, firewalls and other network security tools as appropriate.

24.3. AWS will permit data center operator or other service provider to connect your hardware to AWS's hardware at the AWS Direct Connect location(s) that you select. AWS will provide the necessary information to enable the data center operator or other service provider to establish and monitor this connection, including your name, email address, network configuration, activity information, and AWS account number.

24.4. You are responsible for your separate relationship with the data center operator or other service provider, including compliance with your agreement with, and the policies and procedures of, the data center operator or other service provider, and payment of applicable fees to the data center operator or other service provider. You are responsible for providing or procuring (and AWS will not own) any equipment or cabling necessary to establish this dedicated connection. Neither AWS nor any of its affiliates are responsible for the

24.5. We may disconnect your AWS Direct Connect connection at any time for any reason. If the connection you establish as part of AWS Direct Connect is temporarily unavailable or terminated, AWS will route traffic bound for your AWS resources over the public Internet and AWS's standard data transfer charges will apply. However, if you are using Amazon Virtual Private Cloud (VPC), traffic bound for your Amazon VPC resources will be routed through an IPsec VPN connection. If an IPsec VPN connection is unavailable, traffic bound for your Amazon VPC resources will not be delivered.

25. Amazon ElastiCache

25.1. You may only use Amazon ElastiCache to store, query, retrieve and serve Your Content. You are solely responsible, for the proper configuration of all security settings associated with Amazon ElastiCache.

25.2. You may not access or tamper with any software we install on the cache nodes as part of Amazon ElastiCache.

25.3. Amazon ElastiCache is designed for the ephemeral storage of Your Content. You are responsible for maintaining a persistent data storage for Your Content, and routinely archiving Your Content to prevent the loss of Your Content.

25.4. Replacement cache nodes automatically generated by Amazon ElastiCache may have different IP address, and you are responsible for reviewing your application configuration to ensure that your cache nodes are associated with the appropriate IP addresses.

25.5. We may apply software updates on your behalf if we determine there is a security vulnerability in the system or software we install on the cache nodes as part of Amazon ElastiCache.

25.6. Reserved Cache Node Pricing. You may designate Amazon ElastiCache cache node as subject to the reserved pricing and payment terms (**"Reserved Cache Node Pricing"**) set forth on the Amazon ElastiCache detail page on the AWS Site (each designated instance, a **"Reserved Cache Node"**). You may designate cache nodes as Reserved Cache Nodes by calling to the Purchasing API or selecting the Reserved Cache Node option in the AWS console. When you designate a cache node as Reserved Cache Node, you must designate a region, cache node type, Reserved Cache Node type, and quantity for the applicable Reserved Cache Node. The Reserved Cache Node may only be used in the designated region. We may change Reserved Cache Node Pricing at any time, but price changes will not apply to previously designated Reserved Cache Nodes. We may terminate the Reserved Cache Node Pricing program at any time. Reserved Cache Nodes are nontransferable, and all amounts paid in connection with Reserved Cache Nodes are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved Cache Node type, or terminate the Reserved Cache Node Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved Cache Nodes. Upon expiration or termination of the term of a Reserved Cache Node, the Reserved Cache Node Pricing will expire and standard on-demand usage prices will apply to the cache node. In addition to being subject to Reserved Cache Node Pricing, Reserved Cache Nodes are subject to all data transfer and other fees applicable under the Agreement.

26.1. We will provide "Support" in accordance with the terms of AWS Support Features page available at http://aws.amazon.com/premiumsupport (the **"Guidelines"**). AWS Support is available only as described in the Guidelines. If you are experiencing problems with one or more Services in connection with your use of any Content that was provided to you by a third party (someone other than yourself or AWS) then AWS Support is not available.

26.2. In providing AWS Support, AWS will use commercially reasonable efforts to (a) respond within the "Response Times" set forth in the Guidelines for all properly submitted cases from authorized individuals, and (b) work towards the identification and resolution of the problems submitted. When submitting a case, you may designate the severity level of a problem; provided that, we reserve the right to reclassify the severity level in our reasonable opinion. All Response Times are measured from the point when a case has been properly submitted by an authorized individual to us. Cases may be submitted as specified in the Guidelines. We do not represent, warrant or guarantee that (i) we will always be able to resolve a case fully, (ii) you will no longer experience a problem, (iii) we will provide a bug fix, patch or other workaround in connection with the identified problem, or (iv) any support or advice will result in any performance efficiency or improvement. You are solely responsible for the implementation and results of any suggestions or advice received.

26.3. Unless otherwise set forth in the Guidelines, AWS Support fees will be the greater of (a) the specified minimum monthly fee, or (b) a percentage of your monthly usage charges, calculated before any discounts or credits are applied, for all Services during the billing period. Regardless of when you sign up or terminate AWS Support, you are obligated to pay for a minimum of thirty (30) days of support each time you register to receive the service. Implementation of any suggested configurations or improvements may result in additional fees and charges. We reserve the right to refuse to provide AWS Support to any customer that frequently registers for and terminates the service.

27. AWS GovCloud (US) Service Terms

27.1. You are responsible for satisfying any applicable eligibility requirements for using the AWS GovCloud (US) Region including providing accurate and current registration information. We may require you to provide additional registration information before we permit you to access the AWS GovCloud (US) Region. Such information may include your U.S. person status, as defined by 22 CFR part 120.15 (**"US Person"**), and whether you are subject to export restrictions under U.S. export control laws and regulations. We may make, directly or through third parties, any inquiries we consider necessary to validate information that you provide to us, including without limitation checking commercial and/or governmental databases. While we may take steps to verify the identity of our Customers, we cannot and do not guarantee any Customer's identity.

27.2. AWS is responsible for maintaining access controls to the AWS GovCloud (US) Region that limit AWS personnel's physical and logical access to the "AWS Network" to US Persons only. The AWS Network consists of AWS's internal data center facilities, servers, networking equipment, and host software systems that are within AWS's reasonable control and are used to provide the AWS Services. You are responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, Customer or End User account access, data transmission, encryption, and appropriate storage and processing of your Content within

and their End Users.

27.3. You are responsible for verifying the adequacy of the AWS GovCloud (US) Region for the processing and storage of your Content and that your use of AWS Services will comply with the laws and regulations that may govern your Content. You are also solely responsible for verifying that End Users are eligible to access your Content in the AWS GovCloud (US) region.

27.4. You may only use Amazon VPC to connect your computing resources to the AWS GovCloud (US) region.

27.5. AWS Services may not be used to process or store classified data. If you or your end users introduce classified data into the AWS Network, you will be responsible for all sanitization costs incurred by AWS.

28. Amazon DynamoDB

28.1. You will be charged for the throughput capacity (reads and writes) you provision in your Amazon DynamoDB tables even if you do not fully utilize the provisioned capacity.

28.2. The actual reads and writes performance of your Amazon DynamoDB tables may vary and may be less than the throughput capacity that you provision.

28.3. Reserved Capacity Pricing. You may purchase reserved throughput capacity (reads and writes) subject to the pricing and payment terms set forth on the Amazon DynamoDB detail page on the AWS Site (**"Amazon DynamoDB Reserved Capacity"**). You may purchase Amazon DynamoDB Reserved Capacity by submitting a request through the AWS console. When you purchase Amazon DynamoDB Reserved Capacity, you must designate a region, quantity, and term. You will be charged (1) a one-time, up-front fee and (2) an hourly fee for each hour during the term based on the amount of Amazon DynamoDB Reserved Capacity you purchase. The Amazon DynamoDB Reserved Capacity may only be used in the designated region and only by the account that purchased the Amazon DynamoDB Reserved Capacity. We may change the pricing for Amazon DynamoDB Reserved Capacity at any time, but price changes will not apply to previously purchased Amazon DynamoDB Reserved Capacity. We may terminate the Amazon DynamoDB Reserved Capacity program at any time. Amazon DynamoDB Reserved Capacity is nontransferable and all amounts paid in connection with the Amazon DynamoDB Reserved Capacity are nonrefundable, except that if we terminate the Agreement (other than for cause) or the Amazon DynamoDB Reserved Capacity program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously purchased Amazon DynamoDB Reserved Capacity. Upon expiration or termination of the term of any Amazon DynamoDB Reserved Capacity, standard on-demand usage prices will apply to your use of Amazon DynamoDB. Amazon DynamoDB Reserved Capacity is also subject to all storage, data transfer and other fees applicable under the Agreement.

28.4. You may install the local version of DynamoDB only on computer equipment owned or controlled by you and may use it solely (a) for your internal business purposes and (b) in connection with the Services. Your use of DynamoDB Local is governed by the DynamoDB Local License Agreement, located here: DynamoDB Local License Agreement.

29.1. You may only use the AWS Storage Gateway on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the AWS Storage Gateway is governed by the AWS Storage Gateway License, located here: AWS Storage Gateway License Agreement.

30. AWS Marketplace

30.1. The AWS Marketplace is a venue operated by AWS that allows Content to be offered, sold, and bought. Content may be sold by AWS or a third party, and the party offering or selling the Content may specify separate terms and conditions and privacy policies for the use of the Content. If the Content is offered or sold by a third party, that party will be the seller of record for the Content. AWS is not a party to the terms with respect to Content offered or sold by third parties. Any Content of third parties offered through the AWS Marketplace constitutes "Third Party Content" under the Agreement. While AWS may help facilitate the resolution of disputes between you and third parties, AWS is not responsible for Third Party Content and has no control over and does not guarantee the quality, safety or legality of items advertised, the truth or accuracy of Third Party Content or listings, or the ability of sellers to offer the Content.

30.2. Except to the extent Content is provided to you under a separate license that expressly states otherwise, neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content, (b) reverse engineer, disassemble, or decompile the Content or apply any other process or procedure to derive the source code of any software included in the Content, (c) resell or sublicense the Content, (d) transfer Content outside the Services without specific authorization to do so, or (e) tamper with or circumvent any controls or make unauthorized copies of the Content.

30.3. AWS may stop providing the AWS Marketplace (or any features of or listings within the AWS Marketplace) to you at AWS's sole discretion, without prior notice to you. In addition, AWS may disable or remove Content already purchased, if AWS determines in its sole discretion that the Content may violate any AWS policies or any other regulations, policies or laws.

30.4. You authorize AWS, its affiliates, and its third-party payment processors and any service providers to charge the payment method you select in your AWS account for Content that you purchase in the AWS Marketplace. This may include one-time payments as well as recurring payments. A "recurring payment" is a payment that occurs at the specified intervals and amounts provided at the time of purchase (e.g. annually or monthly). The applicable fees and billing periods for the Content are listed on the confirmation screen when you place your order. Your authorizations will remain until cancelled. You may cancel your subscriptions at any time by logging into "Your Software Subscriptions" on the AWS Site. Unless we specify otherwise, only valid credit cards may be used to purchase a recurring payment subscription.

30.5. If you have provided your value added tax (VAT) registration number to us so that it can be applied to your purchases on AWS, then the information you provide with your registration (including your VAT registration number and the name and address associated with your VAT registration) will be shared with third

30.6. You are responsible for any AWS Marketplace purchases made with your account, which includes third party terms agreed to with your account, even if the purchase was made by an End User through your account.

31. AWS Data Pipeline

31.1. You may only use the AWS Data Pipeline on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services.

31.2. Your use of the AWS Data Pipeline Remote Runner is governed by the AWS Data Pipeline Remote Runner License, located here: AWS Data Pipeline Remote Runner License Agreement.

32. Amazon Elastic Transcoder

32.1. The further distribution of files created by Amazon Elastic Transcoder may require that you obtain license rights from third parties, including owners or licensors of certain third party audio and video formats. You are solely responsible for obtaining these licenses and paying any necessary royalties or fees.

32.2. We do not represent, warrant or guarantee the quality of any files you create through your use of Amazon Elastic Transcoder or that the files will be of a certain fidelity or error free.

33. AWS OpsWorks

33.1. "AWS OpsWorks" means AWS OpsWorks Stacks, AWS OpsWorks for Chef Automate, and AWS OpsWorks for Puppet Enterprise. You may use AWS OpsWorks to create a collection of AWS resources and provision them.

33.2. You may install and use the AWS OpsWorks agent solely with AWS OpsWorks. Your use of the AWS OpsWorks agent is governed by the AWS Opsworks Client License Agreement, located here: AWS OpsWorks Client License Agreement.

33.3. AWS may make sample templates available for you to use in connection with AWS OpsWorks. Sample templates may include Puppet modules, Puppet Tasks, Chef recipes, and/or sample code. All sample templates are offered "as is" and you are solely responsible for your use of the sample templates. Any templates you use in connection with AWS OpsWorks must comply with the Agreement and the AWS Acceptable Use Policy and you are solely responsible for your use of any templates.

33.4. In addition to any charges you incur for your use of AWS OpsWorks, you are responsible for all fees incurred for AWS Services used in connection with AWS OpsWorks.

33.5. AWS OpsWorks for Chef Automate.

33.5.2. In addition to the terms for AWS OpsWorks for Chef Automate, your use of AWS OpsWorks for Chef Automate is also subject to Chef Software Inc.'s end user license agreement, currently located here: https://www.chef.io/aws_eula/.

33.6. AWS OpsWorks for Puppet Enterprise.

33.6.1. By using AWS OpsWorks for Puppet Enterprise, you will create a managed Puppet server and you are responsible for the charges for the Amazon EC2 instance used to run your managed Puppet server.

33.6.2. In addition to the terms for AWS OpsWorks for Puppet Enterprise, your use of AWS OpsWorks for Puppet Enterprise is also subject to Puppet, Inc.'s end user license agreement, currently located here: AWS OpsWorks Client License Agreement.

34. AWS CloudHSM

34.1. You may not access, modify, update or tamper with, or attempt to access, modify, update or tamper with, any of the software installed on the HSM, except as expressly permitted by us.

34.2. As part of the AWS CloudHSM service, AWS will provide access to HSMs of its choosing. You have no ownership or rental rights in the specific HSM to which we provide you access in the course of providing the AWS CloudHSM service.

34.3. In conjunction with the AWS CloudHSM service, you may be allowed to use certain software (including related documentation) developed and owned by SafeNet, Inc. or its licensors (collectively, the **"SafeNet Software"**). If you use the SafeNet Software, SafeNet and its licensors require that you agree to the additional terms and conditions located here.

34.4. Failure of an HSM can result in unrecoverable data loss. We do not implement fault tolerant configurations on your behalf. You are solely responsible for configuring your HSMs in appropriate fault tolerant configurations.

35. Amazon AppStream and Amazon AppStream 2.0

35.1. When you use Amazon AppStream and Amazon AppStream 2.0 (collectively, "AppStream"), you also use Amazon EC2, CloudWatch and AutoScaling, S3, and DynamoDB, and your use of AppStream is subject to all the terms that govern those services.

35.2. The software and other content that you upload to run on AppStream (including your AppStream hosted application, dependencies and installer), your AppStream entitlement service, and your AppStream client software are Your Content. The use of Your Content with AppStream, including the transmission of internet video and your distribution of any video decoder in your AppStream client software, may require that you

35.3. Using Third Party Software. In conjunction with the Services, you may be allowed to use certain software (including related support, maintenance, and documentation) developed, owned or provided by third parties or their licensors. Use of third party software is subject to these additional terms and conditions:

(a) NVIDIA Software. If your application uses the NVIDIA graphics processing unit (GPU) on an AppStream instance, NVIDIA Corporation and its licensors require that you agree to these additional terms and conditions:

Use of the NVIDIA GPU in an AppStream instance requires that you use driver software developed and owned by NVIDIA Corporation or its licensors. Your use of the NVIDIA driver software is subject to the terms and conditions of the License for Customer Use of NVIDIA driver software, currently located at http://www.nvidia.com/content/DriverDownload-March2009/licence.php?lang=us (the "NVIDIA License"). By using the NVIDIA Software, you hereby agree to be bound by the terms of the NVIDIA License.

By using the NVIDIA GPU in an AppStream instance, you are using NVIDIA Corporation's GRID Software, and you agree to be bound by the terms and conditions of the NVIDIA GRID Cloud End User License Agreement located at http://aws-nvidia-license-agreement.s3.amazonaws.com/NvidiaGridAWSUserLicenseAgreement.DOCX.

35.4. We may collect information about Your Content's use of AppStream, including CPU and GPU utilization, memory usage, IO performance, client type, client session length, transmission latency, client geographic and network locations, video and audio quality, and error and information messages.

35.5. AppStream Stand-Alone; AppStream Materials. We may make AppStream software and other materials ("AppStream Materials") available to you on instances running in your own AWS account ("AppStream Stand-Alone"). AppStream Stand-Alone may only be used for your evaluation, development and testing purposes, and not for streaming your application to third party end users. AppStream Stand-Alone may enable you to direct us to pre-install certain third-party software on the instance via the applicable CloudFormation template. That third-party software may be subject to separate license terms and you are solely responsible for complying with those terms. AppStream Materials used on AppStream Stand-Alone are AWS Content and are subject to the license restrictions set out in the Agreement. You will only use the AppStream Materials on the AppStream Stand-Alone instance, and you will not download, transmit, or otherwise remove the AppStream Materials from AppStream Stand-Alone instances.

35.6. If you use the AppStream User Pool feature to enable End Users to access applications, you agree that we may store and process emails associated with such End Users in AWS Regions outside the AWS Regions where you are using AppStream solely in connection with, and for the sole purpose of, sending email notifications to such End Users to enable them to access AppStream and their assigned applications.

36. Amazon WorkSpaces

Content on your WorkSpaces.

36.2. Using Microsoft Software. In conjunction with the Services, you and your End Users may be allowed to use Microsoft Software. If you choose to use the Microsoft Software, Microsoft and its licensors require that you agree to the additional terms and conditions specified in Section 4.2 above.

36.3. You and End Users may only use the WorkSpaces Services for an End User's personal or office productivity. WorkSpaces are not meant to accept inbound network connections, be used as server instances, or serve web traffic or your network traffic. You may not reconfigure the inbound network connections of your WorkSpaces. We may shut down WorkSpaces that are used in violation of this Section or other provisions of the Agreement.

36.4. You and End Users may only use the WorkSpaces client software on computer equipment owned or controlled by you or your End Users for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the WorkSpaces client software is governed by the WorkSpaces Client Software License Agreement located here: WorkSpaces Client Software License Agreement.

36.5. As part of regular operation the Service will be able to perform configurations, health checks, and diagnostics on a regular basis. To complete these tasks the Service will use programmatic access that is provisioned as part of the WorkSpace creation. During the performance of these tasks, the Service may only retrieve performance and log information tied to the operation and management of the Service.

36.6. The charges for the Service apply on a monthly basis. If a WorkSpace is launched after the first of a month, then the monthly price for that WorkSpace will be adjusted on a pro rata basis from the first day it was active to the end of that month. If a WorkSpace is terminated before the end of a month, then the monthly charge will still apply.

36.7. The charges for the Service include the cost of streaming data between your WorkSpaces and End Users' devices unless you stream via VPN, in which case you will be charged VPN data transfer rates in addition to any applicable Internet data transfer changes. Other WorkSpace data transfer will be charged using Amazon EC2 data transfer pricing.

36.8. You may not attempt to tamper with any software we pre-load on the WorkSpace instance (including the operating system software running on the WorkSpace), or in a way that is not part of normal operations or that attempts to circumvent charges for the Service. During the regular operation of the Service, software installed on any of your WorkSpaces may activate against a license activation server hosted by AWS. You may not attempt to tamper with or use this license activation server in a way that is not part of normal operations or that attempts to circumvent charges for the Service. We may block access to the Service, and suspend your account, if we determine that you are in violation of this Section.

36.9. As part of regular operation of the service, WorkSpaces may be updated with latest operating system and software patches. During such updates, only software, documents, and settings that are part of the OS image used for the WorkSpace or part of a user's profile (D: drive in the WorkSpace) will persist.

must be eligible to use the WorkSpaces BYOL Program for the applicable Microsoft software under your agreement(s) with Microsoft. You are solely responsible for obtaining all required licenses and for complying with all applicable Microsoft licensing requirements, including the Product Use Rights/Product Terms. Further, you must have accepted Microsoft's End User License Agreement (Microsoft EULA), and by using Microsoft Software under the WorkSpaces BYOL Program, you agree to the Microsoft EULA. You agree that you have determined that your use of the WorkSpaces BYOL Program will comply with the applicable Microsoft licensing requirements. Usage of the Services in violation of your agreement(s) with Microsoft is not authorized or permitted. AWS recommends that you consult with your own advisors to understand and comply with the applicable Microsoft licensing requirements.

36.11. You are responsible for End Users use of your WorkSpaces. You are responsible for determining End User policies and configuring End User policy controls for WorkSpaces.

37. Amazon Cognito

37.1. Any third party identity provider that you use in connection with Amazon Cognito is Third Party Content under the Agreement, and features of Amazon Cognito that depend on such identity providers may not be secure, uninterrupted or error-free. Your use of such an identity provider is subject to the provider's terms and conditions, and you are solely responsible for complying with those terms and conditions. We may change, discontinue, or deprecate support for an identity provider for any reason and at any time.

37.2. You are responsible for (a) providing legally adequate privacy notices to your end users; (b) obtaining any necessary consent from the end user for the collection, use, transfer, and storage of any name, password, other login information, or personally identifiable information or personal data of any end user that you (or any third-party plug-in or service provider you use) may access; (c) using and authorizing others to access and use the information only for the purposes permitted by the end user; and (d) ensuring the information is collected, used, transferred, and stored in accordance with all laws, rules, and regulations applicable in jurisdictions in which your applications are used.

37.3. Cognito Identity User Pools.

37.3.1. You are solely responsible, and we have no liability, for any activities that result by your use of Cognito User Pools, regardless of whether such activities are undertaken by you, your employees, agents, and/or subcontractors.

37.3.2. You may create Cognito User Pools in association with your AWS Account pursuant to the Terms of this Agreement. You are responsible for the creation and security (including enabling of access) of any Cognito User Pools enabled by your AWS Account. In the event a particular Cognito User Pool(s) has no active users within a reasonable amount of time we may delete in our sole discretion, and without liability of any kind, such Cognito User Pool(s) upon thirty (30) days prior notice to you. You may contact AWS Support if you would like your user data exported to a file prior to deletion.

messages. Your use of Cognito User Pools is subject to the Amazon SNS and SMS Service Terms.

38. Amazon WorkDocs

38.1. Amazon WorkDocs from the Asia Pacific (Tokyo) Region is sold and provided by AMCS LLC and not AWS, but is otherwise subject to the terms of the Agreement.

38.2. You will need an AWS account to start using the Service Offering. Once you have enabled Amazon WorkDocs under your account, End Users can be invited to join, sign up, and start using the Service Offering under your account without each one having a separate AWS account.

38.3. You are responsible for paying the fees for use by you and your End Users of the Service Offering associated with your AWS account.

38.4. Within the Service Offering, your End User accounts are managed by End Users with administrative privileges ("**WorkDocs Administrators**"). These WorkDocs Administrators can access information about the accounts of other End Users, such as when they last logged in, what documents they viewed, etc. These WorkDocs Administrators can also deactivate other End Users' accounts and control access to certain functionality, such as restricting the ability to share files with external domains or changing their storage limits.

38.5. We may limit the number of versions that you can store for each file. We will announce any change in limits to the number of versions that you may store in advance of implementing those limits.

38.6. We may delete, without liability of any kind, any of your End Users' data or Content uploaded to Amazon WorkDocs if the End User is marked "Inactive" in Amazon WorkDocs' Administrator Dashboard and has not been billed for more than 30 days. We may also delete your Amazon WorkDocs site and Content when you have no End Users marked "Active" within Amazon WorkDocs Administrator Dashboard for more than 30 days.

38.7. If no End User accounts associated with your AWS account have registered any usage of the Service Offering for several months, then we may delete the inactive End Users' accounts after providing 30 days' notice.

38.8. You and your End Users may not use the Service Offering to host any files that violate the AWS Acceptable Use Policy. If we determine, in our sole discretion, that your use of the Service Offering may be in violation of the AWS Acceptable Use Policy or the Agreement, then we may delete those files.

38.9. Your use of the Amazon WorkDocs Sync Software is governed by the Amazon WorkDocs Sync License Agreement found here: Amazon WorkDocs Sync License Agreement.

38.10. Your use of an Amazon WorkDocs Application is governed by the Amazon WorkDocs Application License Agreement found here: Amazon WorkDocs Application License Agreement.

38.12. Open with Office 365 is Third Party Content provided by Microsoft. By using Open with Office 365, you are subject to Microsoft's terms of use and privacy policy. You are solely responsible for obtaining all required licenses from Microsoft to use Open with Office 365 and for complying with all applicable Microsoft licensing requirements.

38.13. The Hancom document editing service is Third Party Content. Your use of the Hancom document editing service through the Service Offering is subject to the Hancom Terms of Service. If you do not accept the Hancom Terms of Service applicable to the Hancom document editing service, then do not enable and use the Hancom document editing service. If you enable and use the Hancom document editing service, Hancom will have access to the contents of the document being edited and the End User's user name and profile picture. Hancom is only authorized by AWS to access the above information for the purpose of providing the Hancom document editing service and only for the duration of the editing session.

39. Amazon Pinpoint

39.1. Your Data; Privacy. You are solely responsible for all information and data you collect or store using Amazon Pinpoint ("Your Data"). Your Data is included in the definition of Your Content. Without limiting your obligations under Sections 4 and 9 of the Agreement, you must (a) provide any necessary notice to, and obtain any necessary consent from, End Users for the collection, use, transfer, and storage of Your Data (including by us), and (b) collect, use, transfer, and store Your Data in accordance with any privacy notice you provide, and all applicable laws.

39.2. Amazon Pinpoint utilizes underlying functionality from the Amazon Simple Notification Service (Amazon SNS) and Amazon Simple Email Service (SES), and your use of Amazon Pinpoint is subject to the terms that govern those Services.

39.3. When you use Amazon Pinpoint to send push notifications, you are responsible for: (a) obtaining all necessary certificate(s) and/or license(s) from push notification service providers; and (b) ensuring you have all necessary legal and data privacy terms in place with push notification service providers, including terms necessary to comply with applicable law (including the EU General Data Protection Regulation).

39.4. Mobile Analytics features and functionality are now incorporated into Amazon Pinpoint, and references to Amazon Pinpoint in these Service Terms will include reference to such features and functionality.

40. AWS Config

40.1. You are responsible for all fees incurred for Services, such as Amazon SNS and Amazon S3, used in connection with AWS Config.

41. AWS CodeDeploy

that are posted on the AWS CodeDeploy detail page on the AWS Site; and may also be used with other AWS Services. You are responsible for all fees incurred for Services used in connection with AWS CodeDeploy.

41.2. AWS may make available reference or sample AppSpec configuration files and applications for you to use in connection with AWS CodeDeploy. These files and applications are provided "as is", and you are solely responsible for your use of such files and applications. You will be charged the same fees for running them as you would be charged for running your own application.

42. AWS Lambda

42.1. You are responsible for Your Content, including (a) the performance of software you use with AWS Lambda and any reference libraries we provide and (b) maintaining licenses and adhering to the license terms of any software you run.

42.2. You are responsible for all fees incurred for Services used in connection with AWS Lambda.

42.3. We may delete, upon 30 days' notice to you and without liability of any kind, any of Your Content uploaded to AWS Lambda if it has not been run for more than three (3) months.

43. Amazon WorkMail

43.1. The charges for the Service apply on a monthly basis. If an End User account is created after the first of a month, then the monthly fee for that mailbox will be adjusted on a pro rata basis from the first day it was active to the end of that month. If an End User account is terminated or deleted before the end of a month, then the monthly fee for that End User account will still apply. You are responsible for paying the fees for all End User accounts associated with your AWS account.

43.2. Amazon WorkMail allows you to register a test mail domain (e.g. <yourname>.awsapps.com). You can use the test mail domain as long as you are using Amazon WorkMail. If you stop using Amazon WorkMail, the test mail domain may become available to be registered and used by other Customers. You cannot use the test mail domain for other purposes outside of Amazon WorkMail.

43.3. If your use of Amazon WorkMail is terminated, we may delete your data and your End Users' mailboxes.

43.4. When you use Amazon WorkMail, you also use AWS Key Management Service, AWS IAM, and Amazon SES, and your use of Amazon WorkMail is subject to the terms that govern those services. You are responsible for the separate fees you may accrue for using AWS Key Management Service.

43.5. Amazon WorkMail provides a filtering service designed to filter unwanted emails, such as spam, phishing emails, and email infected with viruses. You acknowledge that the technological limitations of the filtering service will likely result in the capture of some legitimate email, and the failure to capture some unwanted email, including email infected with viruses.

regardless of whether delivery of your emails is prevented, delayed, or blocked.

43.7. You agree not to use Amazon WorkMail for sending:

- Bulk emails, such as mass marketing emails
- Unsolicited and unwanted emails
- Phishing emails

43.8. Your use and your End Users' use of Amazon WorkMail must comply with the AWS Acceptable Use Policy, applicable law, and the Agreement. You are solely responsible for understanding and complying with the legal and regulatory requirements applicable to your business. You are solely responsible for ensuring any emails you or your End Users send using Amazon WorkMail comply with the Federal CAN-SPAM Act and all other applicable law. You agree that AWS is not the "sender" of any emails you or your End Users send using Amazon WorkMail as defined in the Federal CAN-SPAM Act and all other applicable laws.

43.9. Amazon WorkMail may log and use information such as server hostnames, IP addresses, timestamps, mail queue file identifiers, and spam filtering information for the purpose of troubleshooting or improving Amazon WorkMail.

44. Amazon Machine Learning

44.1. You may only use Amazon Machine Learning ("**Amazon ML**") to process Your Content. You are solely responsible for the proper configuration of all security settings associated with Amazon ML.

44.2. We retain all rights to all improvements we make to any Amazon websites or technologies, including any and all improvements resulting from or related to Amazon ML processing Your Content.

44.3. We may delete, without liability of any kind, any Amazon ML object that remains inactive for more than the number of days specified in the user documentation.

44.4. You are responsible for all fees incurred from your use of Amazon ML regardless of the quality of the results obtained. Your use of Amazon ML requires the use of other Services. You are responsible for all fees incurred for Services used in connection with Amazon ML.

45. Amazon WorkSpaces Application Manager (Amazon WAM)

45.1. Any Content that you or any End User run on, cause to interface with, or upload to Amazon WorkSpaces Application Manager (Amazon WAM) via the Amazon WAM Admin Studio is Your Content.

45.2. You are responsible for maintaining licenses and adhering to the license terms of any of Your Content delivered via Amazon WAM to your WorkSpaces.

that is provisioned as part of Amazon WAM. During the performance of these tasks, the Service may only retrieve performance and log information tied to the operation and management of the Service.

45.4. As part of regular operation of Amazon WAM, the Service will use the End User and machine identity that is part of your AWS Directory Services environment to check for content that an End User is entitled to use. In addition, content installed on any of your WorkSpaces may activate against a license activation server hosted by AWS. You may not attempt to tamper with this license activation server, or use it in a way that is not part of normal operations or that attempts to circumvent this Service. We may block access to this Service, and suspend your account, if we determine that you are in violation of this Section.

45.5. The charges for the Service apply on a monthly basis. If Amazon WAM is enabled for an End User after the first of a month, then the monthly price for that End User's subscription will be adjusted on a pro rata basis from the first day it was active to the end of that month. If Amazon WAM is disabled for an End User before the end of a month, then the entire monthly charge will still apply.

45.6. When you use Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications, you may also use other AWS Services, and use of other AWS Services is subject to the terms that govern those Services. In addition to any charges you incur for your use of Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications, you are responsible for all fees incurred for AWS Services used in connection with Amazon WAM, including Amazon WAM Admin Studio and Amazon WAM Admin Player applications.

45.7. Amazon WAM Admin Studio, Amazon WAM Admin Player, and Amazon WAM desktop applications are AWS Content and may not be manipulated or reverse engineered in any way.

45.8. You may use the Amazon WAM Admin Studio only to package applications, and the Amazon WAM Admin Player only to validate applications, that will be delivered via Amazon WAM to your WorkSpaces. You may not tamper with either of those applications that we preload as part of the Amazon WAM Admin Studio or Player, the underlying Amazon EC2 AMI, or use the Amazon WAM Admin Studio or Player in a way that is not part of normal operations or that attempts to circumvent this Service.

45.9. You may not attempt to tamper with any software that is part of the Amazon WAM service that we preload on the WorkSpace instance, or use it in a way that is not part of normal operations or that attempts to circumvent this Service.

45.10. As part of regular operation of the Service, we may update Amazon WAM desktop applications with software patches.

45.11. You are responsible for End Users use of Amazon WAM. You are responsible for determining End User policies and configuring End User policy controls for using applications via Amazon WAM.

46. AWS Marketplace for Desktop Apps

may specify separate terms and conditions and privacy policies for the use of the Content.

46.2. Except to the extent Content is provided to you under a separate license that expressly states otherwise, neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any Content, (b) reverse engineer, disassemble, or decompile the Content or apply any other process or procedure to derive the source code of any software included in the Content, (c) resell or sublicense the Content, (d) transfer Content outside the Services without specific authorization to do so, or (e) tamper with or circumvent any controls or make unauthorized copies of the Content.

46.3. AWS may stop providing the AWS Marketplace for Desktop Apps (or any features of or listings within the AWS Marketplace for Desktop Apps) to you at AWS's sole discretion, without prior notice to you. In addition, AWS may disable or remove Content already purchased, if AWS determines in its sole discretion that the Content may violate any AWS policies or any other regulations, policies or laws.

46.4. You authorize AWS, its affiliates, and its third-party payment processors and any service providers to charge the payment method you select in your AWS account for Content that you purchase in the AWS Marketplace for Desktop Apps. This may include one-time payments as well as recurring payments. A "recurring payment" is a payment that occurs at the specified intervals and amounts provided at the time of purchase (e.g., annually or monthly). The applicable charge for the Content is listed on the confirmation screen when you place your order. Your authorizations will remain until cancelled. If a subscription is purchased after the first of a month, then the monthly price for that Content will be adjusted on a pro rata basis from the first day it was active to the end of that month. If a subscription is cancelled before the end of a month, then the entire monthly charge will still apply. Unless we specify otherwise, only valid credit cards may be used to purchase a recurring payment subscription.

46.5. Third-party support information for each subscription, if any, is set forth on the detail page for the Content. While AWS may help facilitate the resolution of disputes between you and third-party Content creators, for the Content, AWS does not guarantee the quality, safety or legality of items advertised, and support for the Content is the obligation of the third-party Content creator.

46.6. If the Content is offered, sold, or resold by AWS, then it is subject to the terms on the Content's detail page. If the Content is offered or sold by a third party, that party will be the seller of record for the Content. AWS is not a party to the terms with respect to Content offered or sold by third parties. Any Content offered or sold by third parties through the AWS Marketplace for Desktop Apps constitutes "Third Party Content" under the Agreement. While AWS may help facilitate the resolution of disputes between you and third parties, AWS is not responsible for Third Party Content and has no control over and does not guarantee the quality, safety or legality of items advertised, the truth or accuracy of Third Party Content or listings, or the ability of sellers to offer the Content.

47. AWS Directory Service

agree to the additional terms and conditions specified in Section 4.2 above.

47.2. If your AWS account is suspended for sixty (60) days or more, we may delete, without liability of any kind, Your Content and directories that are stored in AWS Directory Service upon thirty (30) days prior notice to you.

47.3. We may terminate your AWS Directory Service directory instance if you attempt to access, tamper with, or modify any software or configuration we pre-load on the directory instance, including the operating system software running on the directory instance.

48. Amazon API Gateway

48.1. You may use the Amazon API Gateway to publish, maintain, monitor, and secure Your Content at any scale to accept and process concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management.

48.2. By using the Amazon API Gateway you acknowledge and agree that established throttling thresholds may vary, cache services may be limited by us in our sole discretion, and version capacity will not exceed 300 deployments per API at any given time. In addition and without limiting your obligations under the Agreement, you agree not to and not to attempt to:

(i) access any resources not assigned to you by us; and/or

(ii) perform any form of network discovery and/or load testing of Your Content inside the Amazon API Gateway.

48.3. You are solely responsible for the access, operation, performance, and security of all Your Content you use with Amazon API Gateway.

49. AWS Device Farm

49.1. As part of the AWS Device Farm, you may provide us with application package(s), test package(s) (pre-compiled), test script source code, application extension files, and/or auxiliary data files that have been developed by or for you in a format specified by AWS (each, an “App” or “Apps”) for testing on one or more mobile devices, tablets or other devices that we make available through the AWS Device Farm (each, a “Device(s)”). You may select one or more tests in the AWS Device Farm to be performed with your App(s) on the Device(s) you select (a “Test” or “Testing”).

49.2. For any Test run on an Apple Device (each, an “Apple Test”), you represent and warrant that you have an active and valid registered Apple Developer Account under the iOS Developer Program License Agreement with Apple at the time any such Apple Test is run. You appoint us as your Authorized Developer (as defined in the iOS Developer Program License Agreement) for the duration of all Apple Tests and understand that you are responsible to Apple for all actions we undertake in connection with each Apple Test.

(i) perform any network discovery inside the AWS Device Farm or otherwise in connection with the Test;

(ii) access any resources not assigned to you by us (including any Devices);

(iii) generate any internet traffic from within the EC2 instances of AWS Device Farm, unless approved by us; internet traffic should be limited to Devices only;

(iv) attempt to establish a direct connection to any Device, nor access or connect to other infrastructure components except as permitted by us;

(v) root, unlock, or jailbreak any Device;

(vi) modify any files generated by the AWS Device Farm in a manner that would interfere with any Services;

(vii) install persistent software on Devices or EC2 instances; and/or

(viii) factory reset or change settings on Devices nor call and/or access third-party servers in a manner that would interfere with any Services.

49.3. You agree not to rely on any Testing or Report for any purpose, including that any App(s) meet any requirements for inclusion in any application repository of any kind (such as the Apple App Store or Google Play Store). You acknowledge and agree that we may disclose the App(s) to third parties solely for purposes of conducting automated security verification.

49.4. We make no representation as to the availability of the AWS Device Farm. We may change the Tests, Reports or Device(s) offering(s) or any other components or services that are a part of or available through the AWS Device Farm at any time.

50. Amazon Elasticsearch Service

50.1. Amazon Elasticsearch Service creates daily automated snapshots of your Amazon Elasticsearch Service domains. We will maintain these automated snapshots for a period of 14 days after they are created. We may delete automated snapshots, without liability of any kind, at any time after 14 days.

50.2. You may not access or tamper with any software we install on the Amazon Elasticsearch Service domains.

50.3. We may apply software updates on your behalf if we determine there is a security vulnerability in the system or software we install on the Amazon Elasticsearch Service domains.

51. AWS Database Migration Service and AWS Schema Conversion Tool

Amazon S3, or relational databases deployed on Amazon EC2 (collectively, as supplemented by AWS from time to time, the "DMS Supported Services"). Neither you nor any End User may use the AWS Database Migration Service to migrate data, directly or indirectly, from a source that is not a DMS Supported Service to a destination that is also not a DMS Supported Service.

51.2. AWS Database Migration Service and the AWS Schema Conversion Tool collect non-personally identifiable metrics regarding your use of the Service Offerings, including the types of database engines used, number of rows processed, duration of the migration or conversion tasks, and migration or conversion task failure status. These metrics may be used by AWS to provide, maintain, and improve the quality and feature set of the Service Offerings.

51.3. The AWS Schema Conversion Tool is AWS Content, and you may install and use it solely for the purpose of migrating your database schemas to Amazon RDS, Amazon Redshift, or relational databases deployed on Amazon EC2 (collectively, as supplemented by AWS from time to time, the "SCT Supported Services"). Neither you nor any End User may distribute the AWS Schema Conversion Tool or use it to migrate database schemas to a destination that is not an SCT Supported Service. If you would like to use the AWS Schema Conversion Tool to migrate database schemas to a destination that is not an SCT Supported Service, contact us for special pricing.

52. Amazon Inspector

52.1. Amazon Inspector, the Amazon Inspector Agent, and any components or files thereof are AWS Content subject to the license restrictions set out in the Agreement. Neither you nor any End User may, or may attempt to, distribute Amazon Inspector.

52.2. Some components of Amazon Inspector are governed by open source software licenses identified in the notice file accompanying the Amazon Inspector Agent. Your license rights with respect to these individual components are defined by the applicable open source software license.

52.3. As part of your use of Amazon Inspector, you will need to install the Amazon Inspector Agent on your EC2 instance(s). As with any interaction between software and a host, this process may result in the termination or replacement of your Amazon EC2 resources due to failure, retirement or other AWS requirement(s). We have no liability whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from the foregoing.

52.4. We may apply software updates on your behalf to the Amazon Inspector Agent if we determine there is a security vulnerability in or a need to update the system or software we install for the Amazon Inspector Agent.

52.5. Amazon Inspector may retain and use information collected by the Amazon Inspector Agent for up to 30 days for the purpose of troubleshooting or improving Amazon Inspector.

or altered based on recommendations made by Amazon Inspector will be of a certain fidelity, error free, or comply with a particular security standard.

53. AWS Amplify

53.1. AWS Amplify can be used to connect to other AWS Services as set forth in the Documentation. You are responsible for all fees incurred for AWS Services that you use in connection with AWS Amplify. You are responsible for maintaining licenses and adhering to the license terms of any software you download and use in connection with AWS Amplify. You must own or have all necessary rights to use any domain name that you use in conjunction with AWS Amplify.

54. AWS IoT

54.1. AWS IoT Services that you enable must comport with AWS IoT Developer Guidelines and this Agreement. AWS Developer IoT Guidelines are subject to change at any time without notice.

54.2. The following data guidelines currently apply to Registry and Shadow Data (as referenced in the AWS IoT Developer Guidelines) stored in connection with individual devices and may be changed at any time without notice. Device Shadow Data for an individual device expires and will be deleted if you do not update the Shadow Data for an individual device within 1 year (12 months). Device Registry Data for an individual device expires and will be deleted if you do not update the Registry data for an individual device within 7 years (84 months). Once the Registry and/or Shadow Data has been updated for an individual device the data restriction time frame for an individual device resets and the Registry and/or Shadow Data storage time frame for an individual device starts over.

54.3. You are responsible for all applicable fees associated with use of the Services in connection with AWS IoT. You are solely responsible, and we have no liability, for any activities that occur in the application and/or use of AWS IoT, regardless of whether such activities are undertaken by you, your employees, agents, subcontractors or customers, or any other third party. You are responsible for the creation, distribution, and security (including enabling of access) of any AWS IoT devices enabled by your AWS account.

54.4. You may use the Code Signing feature only with AWS IoT Device Management. We currently support Code Signing of Your Content utilizing the following software: Amazon FreeRTOS libraries.

55. Amazon QuickSight

55.1. You may enable End Users to use Amazon QuickSight under your account. Termination of your use of Amazon QuickSight, will also terminate such End Users' use of Amazon QuickSight.

55.2. Amazon QuickSight End User accounts are managed by End Users with administrative privileges ("Amazon QuickSight Administrators"). Amazon QuickSight Administrators can (a) activate and deactivate End

55.3. Amazon QuickSight may use Your Content to make personalized recommendations to you, such as suggested visualizations based on your query history.

55.4. Subject to the Agreement and these Service Terms, you and your End Users may use Amazon QuickSight by logging into quicksight.aws.amazon.com.

56. AWS Certificate Manager

56.1. By using AWS Certificate Manager ("ACM") you authorize us, Amazon Trust Services, LLC ("ATS"), or our affiliates (collectively, "Amazon CA") to apply for and obtain publicly trusted SSL/TLS certificates (each, a "Certificate") from certification authorities located in the United States, some of whom may be third parties, for the domain name you provide to us. By submitting a request for a Certificate, you certify that (1) you are the Domain Name Registrant (as defined in the then current CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (the "CA/B Forum Requirements" currently located at https://cabforum.org/baseline-requirements-documents/)); (2) you have control over the Fully-Qualified Domain Name (as defined in the CA/B Forum Requirements); or that (3) you have been granted authority by the Domain Name Registrant to authorize Amazon CA to apply for and obtain each Certificate. You acknowledge that, solely for purposes of obtaining the Certificate and for no other purposes, you are giving Amazon CA control over the Fully-Qualified Domain Name, and you approve of it requesting the Certificate for the domain name. We may decline to provide you with a Certificate for any reason.

56.2. You agree that:

(i) All information you provide in connection with your use of Certificates is and will be accurate and complete information at all times (and you will promptly notify us if your information changes);

(ii) You will review and verify the Certificate contents for accuracy;

(iii) You may use a Certificate provided to you by us solely on servers that are accessible at the subjectAltName(s) listed in the Certificate and will use the Certificate solely in compliance with all applicable laws;

(iv) You will promptly cease using a Certificate, and promptly notify us, in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;

(v) You will promptly cease using a Certificate, and promptly notify us, if the private key associated with the Certificate is, or becomes, subject to a Key Compromise (as defined in the CA/B Forum Requirements) or the Certificate is otherwise subject to misuse;

(vi) You will promptly respond to Amazon CA's instructions concerning Key Compromise or Certificate misuse;

(viii) You will not, in connection with use of the Certificate, upload or distribute any files or software that may damage the operation of another's computer;

(ix) You will not make representations about or use a Certificate except as may be allowed in ATS's CPS;

(x) You will not, in connection with use of the Certificate, impersonate or misrepresent your affiliation with any entity;

(xi) You will not permit an entity other than Amazon CA to control the Private Key matching the Public Key in the Certificate (where "Private Key" and "Public Key" are defined by the CA/B Forum Requirements);

(xii) You will not use a Certificate to breach the confidence of a third party or to send or receive unsolicited bulk correspondence; and

(xiii) Notwithstanding anything to the contrary in the Agreement, you acknowledge that Amazon CA (or our applicable third-party contractor) may revoke a Certificate at any time, and you agree that you will cease using the Certificate immediately upon our notice of such revocation.

57. Amazon Lumberyard Engine

57.1. Lumberyard Materials. Amazon Lumberyard consists of an engine, integrated development environment, and related assets and tools we make available at aws.amazon.com/lumberyard/downloads or otherwise designate as Lumberyard materials (collectively, "Lumberyard Materials"). The Lumberyard Materials include the "Lumberyard Redistributables" listed at docs.aws.amazon.com/console/lumberyard/userguide/lumberyard-redistributables. Lumberyard Materials are AWS Content. The term "Lumberyard Materials" does not include Content distributed with the Lumberyard Materials under separate license terms (such as code licensed under an open source license).

57.2. License. In addition to the rights granted to AWS Content under the Agreement, we also grant you a limited, non-exclusive, non-sublicensable (except to End Users as provided below), non-transferrable license to do the following during the Term:

(a) Development: You may use, reproduce, modify, and create derivative works of the Lumberyard Materials to develop and support video games, software, audio-visual works, and other content (each work created through use of the Lumberyard Materials is a "Lumberyard Project"). Lumberyard Projects, excluding any AWS Content and Third Party Content included therein, are Your Content.

(b) Distribution to End Users: You may use, reproduce, modify, create derivative works of, publicly display, publicly perform, and distribute (including via third party distributors) to End Users the Lumberyard Redistributables (including any permitted modifications and derivatives) as part of a Lumberyard Project. However, you may do so only if (i) the Lumberyard Project provides material

usable by End Users, (iii) you do not distribute in source code form Lumberyard Redistributables that we make available in file formats that are commonly compiled (e.g., C, C++) or for which we make a compiler available, and (iv) you ensure End Users are subject to terms no less protective of the Lumberyard Materials than these Service Terms, including this Section and Sections 57.4 and 57.5 below. You may sublicense these rights, subject to the restrictions in these terms, to your End Users to allow them to use, modify, create new content for, and redistribute your Lumberyard Project (e.g., create new items or levels for a game).

(c) Collaboration with other AWS Customers. You may reproduce and distribute (but not sublicense) the Lumberyard Materials (including any permitted modifications and derivatives): (i) to other AWS customers that are contractors of yours solely for the purpose of allowing those AWS customers to perform work on your behalf, (ii) to other AWS customers in connection with work you perform for them as a contractor, and (iii) to up to 5 other AWS customers who you authorize to distribute a Lumberyard Project in connection with your sale or licensing of that Lumberyard Project (e.g., publishers of a game you develop). Those other AWS customers' rights to the Lumberyard Materials are governed by their agreement(s) with us.

(d) Lumberyard Git Repository. We may make available certain Lumberyard Materials on the "Lumberyard Git Repository" at https://github.com/aws/lumberyard. You may reproduce and distribute to other AWS Customers, via the Lumberyard Git Repository, your modified version(s) of those Lumberyard Materials (your "LM Fork(s)"), subject to any policies we may establish for the Lumberyard Git Repository. Your LM Fork must comply with the Agreement (including these terms); for example, it may not enable Lumberyard Projects to use, or read or write data to or from, Alternate Web Services. You must include a notice stating that the LM Fork is subject to these terms (such as a copy of the License.txt file from the root directory of the Lumberyard Materials). If you obtain an LM Fork from the Lumberyard Git Repository, you are responsible for ensuring that any Lumberyard Project you create with it complies with these terms. If your LM Fork violates the Agreement, then it infringes our copyright in the Lumberyard Materials and we may remove it from the Lumberyard Git Repository and take other actions, including terminating your license to the Lumberyard Materials. "Alternate Web Service" means any non-AWS web service that is similar to or can act as a replacement for the services listed at docs.aws.amazon.com/console/lumberyard/userguide/alternate-web-services.

57.3. No License Fee. There is no fee for the licenses granted in Section 57.2. Other Service Offerings and Third Party Content made available in connection with the Lumberyard Materials may be subject to separate charges and governed by additional terms.

57.4. Operating Restrictions. Without our prior written consent, (a) the Lumberyard Materials (including any permitted modifications and derivatives) may only be run on computer equipment owned and operated by you or your End Users, or on AWS Services, and may not be run on any Alternate Web Service and (b) your Lumberyard Project may not read data from or write data to any Alternate Web Service.

57.5. Other Restrictions. Without limiting the license restrictions set out in the Agreement, you may not (a) distribute the Lumberyard Materials in source code form, except as expressly permitted by Section 57.2(b) and

Lumberyard Materials or any portion thereof as part of a logo or trademark, (d) remove, obscure, or alter any proprietary rights notices (including copyright and trademark notices) contained in the Lumberyard Materials, (e) take any action that would require us or you to license, distribute, or otherwise make available to anyone the Lumberyard Materials under different terms (e.g., combining Lumberyard Materials with software subject to "copyleft" open source licenses), or (f) use or exploit the Lumberyard Materials or any portion thereof in any manner or for any purpose other than as expressly permitted by these terms.

57.6. Registration; Release. Before distributing your Lumberyard Project to End Users, you must register it at aws.amazon.com/lumberyard/registration. You must obtain our prior written consent if the initial public or commercial release of your Lumberyard Project is based on a version of the Lumberyard Materials more than 5 years old.

57.7. Credit. You must credit us in Lumberyard Projects in accordance with the guidelines located at aws.amazon.com/lumberyard/logo-guidelines. AWS Marks included in the Lumberyard Materials may only be used in accordance with the Trademark Use Guidelines. We may use excerpts of publicly released promotional material from your Lumberyard Projects and related trademarks, service marks, trade names, and logos in connection with our marketing, advertisement, and promotion of Lumberyard.

57.8. Forums; Submissions. In addition to your rights to distribute LM Forks on the Lumberyard Git Repository set out above, when discussing Lumberyard Materials in our forums or elsewhere, you may include up to 50 lines of source code from the Lumberyard Materials for the sole purpose of discussing that code. You must identify us as the source of the code. "Lumberyard Submissions" are content relating to Lumberyard Materials (including LM Forks) that you post or otherwise submit to developer discussion sites, sample code repositories, or other AWS or public forums. You grant (i) us a non-exclusive, worldwide, perpetual, irrevocable, transferrable, sublicensable, royalty-free, and fully paid up license under all intellectual property rights to your Lumberyard Submissions, and (ii) other AWS customers the same rights to your Lumberyard Submissions as these Service Terms provide to the Lumberyard Materials. You represent and warrant that you have all necessary rights to grant the license above, and that your Lumberyard Submissions do not infringe the intellectual property rights of any third party or violate this Agreement.

57.9. Data Collection. The Lumberyard Materials may provide us with information about the use of the Lumberyard Materials, including information about system and server resources, features used in the integrated development environment, frequency and duration of use, geographic and network locations, and error and information messages.

57.10. Acceptable Use; Safety-Critical Systems. Your use of the Lumberyard Materials must comply with the AWS Acceptable Use Policy. The Lumberyard Materials are not intended for use with life-critical or safety-critical systems, such as use in operation of medical equipment, automated transportation systems, autonomous vehicles, aircraft or air traffic control, nuclear facilities, manned spacecraft, or military use in connection with live combat. However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization.

Agreement for convenience, your rights in Lumberyard Materials then in your possession survive termination with respect to any previously registered Lumberyard Project. Otherwise, upon termination, you must cease all use, distribution, and other exploitation of the Lumberyard Materials (and any modifications and derivatives).

58. Amazon GameLift

58.1. Your Content. You are solely responsible for Your Content, including (a) the performance of software you use with Amazon GameLift and (b) maintaining licenses and adhering to the license terms of any software you run.

58.2. Other Services. When you use Amazon GameLift, you are also using Amazon EC2. Amazon EC2 and certain other Service Offerings and Third Party Content made available via Amazon GameLift are subject to separate charges and governed by additional terms.

58.3. Use Limitation. Amazon GameLift is designed for hosting interactive video game servers. You may not access or use Amazon GameLift for workloads other than video game server hosting.

58.4. Inactivity. We may delete, upon 30 days' notice to you and without liability of any kind, any of Your Content uploaded to Amazon GameLift if it has not been run for more than 3 months.

58.5. Your GameLift Data. Amazon GameLift may enable you to collect information and data from your End Users ("Your GameLift Data"). Your GameLift Data is included in the definition of Your Content. Without limiting your obligations under Sections 4 and 9 of the Agreement, you must (a) provide any necessary notice to, and obtain any necessary consent from, end users for the collection, use, transfer, and storage of Your GameLift Data, and (b) collect, use, transfer, and store Your GameLift Data in accordance with any privacy notice you provide and all applicable laws.

58.6. Amazon GameLift Local. You may install and use Amazon GameLift Local only on computer equipment owned or controlled by you, solely for your internal business purposes for development and testing (not hosting) of your game in connection with your planned use of Amazon GameLift. Your use of Amazon GameLift Local is governed by the Amazon GameLift Local License Agreement, located at https://aws.amazon.com/gamelift-local-license.

58.7. Amazon GameLift Spot Instance Pricing. You may request that certain Amazon GameLift instances run pursuant to the Amazon GameLift Spot instance pricing and payment terms ("GL Spot Instance Pricing") set forth on the Amazon GameLift product detail page on the AWS Site (each requested instance, a "GL Spot Instance"). GL Spot Instances are sourced from the Amazon EC2 Spot Instance service. We set the price for GL Spot Instances (the "GL Spot Price"), which may vary over time based on a number of factors, including the amount of available compute capacity we have available and the price customers are willing to pay for Amazon EC2 Spot Instances. While a requested GL Spot Instance remains running, you will be charged the current GL Spot Price in effect at the beginning of each instance hour. We may terminate, stop, or hibernate

whatsoever for any damages, liabilities, losses (including any corruption, deletion, or destruction or loss of data, applications or profits), or any other consequences resulting from our termination, stoppage, or hibernation of any GL Spot Instance. GL Spot Instances may not be used with certain Services, features and third-party software we specify, including those listed in Section 4.4, above.

59. AWS Application Discovery Service

59.1. The AWS Application Discovery Service requires installation and use of AWS Connector, and you agree to adhere to the AWS Connector terms in connection with your use of AWS Connector and the AWS Application Discovery Service, its agent, and its components.

59.2. You agree that you have the right to collect and provide, and you consent to the collection and provision of, the data collected by the AWS Application Discovery Service, its agent, and its components ("Discovery Information"), and the transmission to and processing and use by AWS of the Discovery Information in connection with the Service Offerings (as defined in the Agreement). Discovery Information includes information about your software packages; system, equipment, and application configuration, processes and performance; network configurations, communications and dependencies; relationships between the foregoing; and information about the installation and operation of the AWS Application Discovery Service, its agent, and its components.

59.3. You are responsible for determining compliance and complying with the terms of any third party software you use, including any software that interfaces with the AWS Application Discovery Service, its agent, and its components, in connection with your use of the AWS Application Discovery Service.

60. AWS Professional Services

60.1. "AWS Professional Services" are advisory and consulting services that help you use the other Services. If AWS provides AWS Professional Services to you, then this Section 60 will apply. References to "Services" in the Agreement include AWS Professional Services.

60.2. To receive AWS Professional Services, you must enter into a statement of work for each engagement, which will describe the scope of AWS Professional Services to be provided, applicable charges and any applicable additional terms and conditions (each statement of work, a "SOW"). Each SOW is made part of the Agreement. AWS or any of its affiliates may enter into SOWs with you. For the purposes of a SOW, references to "AWS" in the SOW and the Agreement mean references to the AWS entity that enters into the SOW. No AWS entity other than the AWS entity that enters into the SOW has any obligations under such SOW. Any SOW (together with the Agreement as amended by such SOW) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement and supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to such subject matter. If there is a conflict between a SOW and this Section 60, and the SOW explicitly states that it intends to modify the conflicting terms, then the SOW will control.

Professional Services are in addition to any applicable fees for your use of the other Services. AWS will invoice you monthly for the AWS Professional Services and you must pay all invoiced amounts in accordance with the terms of the Agreement. Payments for AWS Professional Services are not refundable.

60.4. You acknowledge that AWS does not provide legal or compliance advice. You are responsible for making your own assessment of your legal and regulatory requirements and whether your use of the Services meets those requirements.

60.5. As stated in the Agreement, you are solely responsible for your use of Third Party Content, and this includes any Third Party Content recommended by AWS. Other than Third Party Content, Content that AWS provides as part of the AWS Professional Services is "AWS Content." You are solely responsible for testing, deploying, maintaining and supporting Content provided or recommended by AWS.

60.5.1. AWS may make Content consisting of either (a) documents and diagrams ("Documents") or (b) software (in source or object code form), sample code, or scripts ("Software") for you as part of the AWS Professional Services (such Documents and Software, "Developed Content"). Subject to any non-disclosure agreement in effect between you and AWS, AWS is not precluded from developing, using, or selling products or services that are similar to or related to the Developed Content. Any Developed Content provided to you by AWS as part of the AWS Professional Services under a SOW is licensed under the following terms:

• AWS licenses any Documents to you under the Creative Commons Attribution 4.0 International License (CC-BY 4.0); and

• AWS licenses any Software to you under the Apache License, Version 2.0.

60.5.2. Some Developed Content may include AWS Content or Third Party Content provided under a separate license. In the event of a conflict between Section 60.5.1 and any separate license, the separate license will prevail with respect to such AWS Content or Third Party Content.

60.6. Any materials or information that you own or license from a third party that is provided to AWS for the purposes of the AWS Professional Services are "Your Content." If you choose to provide access to Your Content to AWS, then you will ensure that you have adequate rights and permissions to do so.

60.7. To the extent that there is a conflict between this Section 60 and any AWS Implementation Services Addendum between you and AWS, the terms of the AWS Implementation Services Addendum will control, and references to "Implementation Services" in that addendum include "AWS Professional Services."

61. Amazon Redshift

61.1. Reserved Node Pricing. You may designate Amazon Redshift nodes as subject to the reserved pricing and payment terms ("Reserved Node Pricing") set forth on the Amazon Redshift pricing page on the AWS Site (each designated node, a "Reserved Node"). You may designate a node as a Reserved Node by calling to the

applicable Reserved Node. The Reserved Node may only be used in the designated region. We may change Reserved Node Pricing at any time, but price changes will not apply to previously designated Reserved Node. We may terminate the Reserved Node Pricing program at any time. Reserved Node are non-cancellable, and you will owe the Reserved Node Pricing for the duration of the term you selected, even if the Agreement is terminated. Reserved Nodes are nontransferable, and all amounts paid in connection with Reserved Nodes are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved Node type, or terminate the Reserved Node Pricing program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved Node. Upon expiration or termination of the term of a Reserved Node, the Reserved Node Pricing will expire and standard on-demand usage prices will apply to the Amazon Redshift node. In addition to being subject to Reserved Node Pricing, Reserved Nodes are subject to all data transfer and other fees applicable under the Agreement.

62. AWS Server Migration Service

62.1. AWS Server Migration Service requires installation and use of AWS Connector, and you agree to the AWS Connector terms in connection with your use of AWS Connector and the AWS Server Migration Service and its associated software and components.

62.2. You acknowledge that the virtual machine image(s) imported in connection with the AWS Server Migration Service will be converted to an Amazon Machine Image and the service will then delete the original version of the imported virtual machine image(s).

62.3. You consent to the collection and provision of the data collected by the AWS Server Migration Service and its associated software and components, including information about your virtual machine image(s); software packages; system, equipment, and application configuration, processes and performance; network configurations, communications and dependencies; relationships between the foregoing; and information about the installation and operation of the AWS Server Migration Service and its associated software and components ("Migration Information"). Migration Information may be used to operate, maintain, and improve the quality and feature set of the Service Offerings.

62.4. You must comply with the terms of any third party services and Third Party Content that you use in connection the AWS Server Migration Service and its associated software and components.

62.5. You acknowledge that the AWS Server Migration Service is designed to migrate virtual machine images and you shall not use the AWS Server Migration Service for ongoing offsite backup or replication. We may terminate the migration of any image that remains in a migration queue for ninety (90) days or more at our discretion.

63. AWS Organizations

63.1. AWS Organizations enables you to (i) create an "Organization" by joining a single AWS account (the "Master Account") with one or more AWS accounts (each, a "Member Account"), and (ii) enable only

Organization. By joining an Organization as a Member Account, you agree to disclose your billing, account activity, and account information of the Member Account to the Master Account.

63.2. Consolidated Billing. By only enabling consolidated billing, the Master Account will pay all applicable charges for its Organization's Member Accounts in accordance with the Master Account's Agreement. If a Master Account is suspended for non-payment, then all Member Accounts in the Organization will be suspended. Master Accounts and Member Accounts are jointly and severally liable for all fees accrued by Member Accounts while the AWS accounts are joined in an Organization. Member Accounts agree that AWS may enable all features in their Organization at the request of their Organization's Master Account with at least 14 days' notice to you that may be sent by email. Member Accounts further agree that their Organization's Master Account may purchase EC2 Reserved Instances on the Member Account's behalf, and the Master Account and Member Account are jointly and severally liable for any fees owed for the Reserved Instances for the term of the Reserved Instances.

63.3. All Features. If your Organization has all features enabled, (i) the consolidated billing terms as described in Section 63.2 will apply to your Organization; (ii) the Master Account will have full access to and control over its Member Accounts; and (iii) the Master Account is jointly and severally liable for any actions taken by its Member Accounts.

63.4. Created accounts. When a Master Account uses AWS Organizations or the CreateLinkedAccount API to create an account ("Created Account"), the Master Account and each Created Account agree as follows: (i) each Created Account will be a member of the Master Account's Organization with the AWS Organizations features that the Master Account enables from time to time; (ii) except as authorized by AWS, each Created Account is governed by the terms of the Master Account's Agreement; and (iii) the Master Account is jointly and severally liable for any actions taken by its Created Accounts. Upon account creation, an IAM role is created in the Created Account that grants the Master Account full administrative access to the Created Account.

64. Amazon Athena

64.1. Notwithstanding any other provision of the Agreement, you may incorporate into your programs or applications, and distribute as incorporated in such programs or applications, the Amazon Athena JDBC Driver or the Amazon Athena ODBC Driver, in each case solely for use with Amazon Athena.

65. Amazon AI Services

65.1. "Amazon AI Services" include Amazon Comprehend, Amazon Comprehend Medical, Amazon Forecast, Amazon Lex, Amazon Personalize, Amazon Polly, Amazon Rekognition, Amazon Textract, Amazon Transcribe, and Amazon Translate. "AI Content" means Your Content that is processed by an Amazon AI Service.

65.2. You will not, and will not allow any third-party to, use the Amazon AI Services to, directly or indirectly, develop or improve a similar or competing product or service. The foregoing does not apply to Amazon Forecast and Amazon Personalize.

processed by each of the foregoing Amazon AI Services to maintain and provide the applicable Amazon AI Service (including but not limited to development and improvement of such Amazon AI Service) and to develop and improve AWS and affiliate machine-learning and artificial-intelligence technologies; and (b) solely in connection with the usage and storage described in clause (a), we may store such AI Content in an AWS region outside of the AWS region where you are using such Amazon AI Service. For the avoidance of doubt, this Section does not apply to Amazon Comprehend Medical.

65.4. You are responsible for providing legally adequate privacy notices to End Users of your products or services that use any Amazon AI Service and obtaining any necessary consent from such End Users for the processing of AI Content and the storage, use, and transfer of AI Content as described under this Section, including but not limited to providing any required notices and obtaining any required verifiable parental consent under the Children's Online Privacy Protection Act (COPPA) or similar laws and obtaining any required consent of individuals appearing in any images or videos processed by an Amazon AI Service. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents. You are responsible for notifying us in the event that any AI Content stored by an Amazon AI Service must be deleted under applicable law. If you use Amazon Lex in connection with websites, programs or other applications that are directed or targeted, in whole or in part, to children under age 13 and subject to COPPA or similar laws you must: (a) provide all required notices and obtain all required verifiable parental consent under COPPA or similar laws; and (b) notify AWS during the Amazon Lex set-up process using the appropriate (i) check box in the AWS console or (ii) boolean parameter in the applicable Amazon Lex Model Building Service API request or response as specified by the Amazon Lex Documentation. Amazon Lex does not store or retain voice or text utterance information from websites, programs, or other applications that you identify in accordance with this Section as being directed or targeted, in whole or in part, to children under age 13 and subject to COPPA or similar laws.

65.5. The distribution of output files created by Amazon AI Services may require that you obtain license rights from third-party owners or licensors of content that you include in AI Content. You are solely responsible for obtaining these licenses and paying any necessary royalties or fees.

65.6. Amazon AI Services are not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious body injury or death or cause environmental or property damage, and you are solely responsible for liability that may arise in connection with any such use.

65.7. Notwithstanding any other provision of the Agreement, you may incorporate into your programs or applications, and distribute as incorporated in such programs or applications, the binary code that we distribute for Amazon AI Services with the AWS Mobile SDKs.

65.8. You and your End Users are solely responsible for any decisions made, advice given, actions taken, and failures to take action based on your use of Amazon AI Services.

66. Amazon Lightsail

66.2. Amazon Machine Images from the AWS Marketplace are offered or sold under the terms of the AWS Marketplace and any separate terms and conditions and privacy policies specified by the party offering or selling the Amazon Machine Image.

66.3. You may not use Amazon Lightsail in a manner intended to avoid incurring data fees from other Services (e.g., proxying network traffic from Services to the public Internet or other destinations or excessive data processing through load balancing Services as described in the Documentation), and if you do, we may throttle or suspend your data services or suspend your account.

66.4. Use of Microsoft Software on Amazon Lightsail is subject to Section 4.2 above.

67. AWS Systems Manager

67.1. Some functionalities of AWS Systems Manager and its associated software and components ("Systems Manager") require installation and use of Amazon SSM Agent and its associated software and components ("Amazon SSM Agent"). These terms for Systems Manager apply to your use of Amazon SSM Agent.

67.2. You must comply with the terms of any third party services and Third Party Content that you use in connection with Systems Manager and Amazon SSM Agent.

67.3. Systems Manager may collect and transmit to AWS information regarding your use of the Service Offerings, including inventory items (e.g., application inventory and custom inventory items); parameters; configuration data (e.g., network and state configuration); telemetry and diagnostics data; update history and registry keys; resource groups; and patch metadata ("Systems Information"). Systems Information may be used by AWS to operate, maintain, and improve the quality and feature set of the Service Offerings.

68. AWS CodeBuild

68.1. Based on your configuration selections within AWS CodeBuild, you may use other Services, such as Amazon S3, CloudWatch Events, Cloudwatch Logs, Simple Notification Service, KMS, and EC2 Container Registry, and your use of those Services are subject to all the terms that govern those Services. You are responsible for all fees incurred for Services used in connection with your use of AWS CodeBuild.

68.2. AWS may make available reference or sample BuildSpec configuration files and applications for you to use in connection with AWS CodeBuild. These files and applications are provided "as is," and you are solely responsible for your use of such files and applications. You will be charged the same fees for running them as you would be charged for running your own application.

69. AWS X-Ray

limiting your obligations under Sections 4 and 9 of the Agreement, you must (a) provide any necessary notice to, and obtain any necessary consent from, end users for the collection, use, transfer, and storage of Your X-Ray Data (including by us), and (b) collect, use, transfer, and store Your X-Ray Data in accordance with any privacy notice you provide, and all applicable laws.

70. Amazon Chime

70.1. End Users.

(a) You may enable End Users to use Amazon Chime under your account. Termination of your account's use of Amazon Chime will also terminate such End Users' Pro tiers, Voice Connector features, and Business Calling features associated with your account or organization and all such End Users will be converted to the Free tier.

(b) Amazon Chime End Users can be managed by End Users with administrative privileges ("Amazon Chime Administrators"). Amazon Chime Administrators can (a) upgrade or downgrade End Users' Amazon Chime tier and feature set; (b) suspend End User's access to Amazon Chime; and (c) access information about End Users' use of Amazon Chime, including, but not limited to, call details.

70.2. PSTN Service.

(a) The term "PSTN Service" as used in these Terms means the ability for you to integrate Public Switched Telephone Network (PSTN) calling and text messaging features into your Amazon Chime experience.

(b) PSTN Service includes (a) dial in access to meetings from the PSTN via standard toll numbers and toll-free numbers; (b) dial out access from meetings to PSTN numbers via standard toll or toll-free numbers; (c) dial in access to Amazon Chime softphones from the PSTN via standard toll or toll-free numbers; (d) dial out access from the Amazon Chime softphone to the PSTN via standard toll or toll-free numbers; (e) receive text and multi-media messages in Amazon Chime messaging via standard toll or toll-free numbers; (f) send text and multi-media messages from Amazon Chime messaging via standard toll or toll-free numbers; (g) dial in access to Amazon Chime Voice Connector from the PSTN via standard toll or toll-free numbers; (h) dial out access from the Amazon Chime Voice Connector to the PSTN via standard toll or toll-free numbers; (i) dial in access to APIs from PSTN via toll or toll-free phone numbers; (j) dial out access from APIs to the PSTN via standard toll or toll-free numbers; (k) receive text and multi-media messages to APIs via standard toll or toll-free numbers; and (l) send text and multi-media messages from APIs via standard toll or toll-free numbers.

(c) Portions of PSTN Service, specifically Business Calling, Voice Connector, and SMS Text, is sold and provided by AMCS LLC ("AMCS") and not AWS, but is otherwise subject to the terms of the Agreement. Your invoice will clearly state which services that you have used are sold to you by AMCS and which are sold by AWS. The invoicing for PSTN Service is performed by AWS on behalf of AMCS for administrative convenience. You do not have to purchase any AMCS services or PSTN Service to use Amazon Chime,

provider and does not itself provide any telecommunications-related services.

(d) By using the PSTN Service, you acknowledge and agree that the following behavior is prohibited: (i) the PSTN Service must not be used in any manner that may expose AWS, its affiliates, or their personnel to criminal or civil liability; (ii) resale of the PSTN Service; (iii) calling or texting PSTN telephone numbers (whether singly, sequentially or automatically) to generate income for you or others as a result of placing the call or texting, other than for your or your End Users' individual business communications, or (iv) unusual calling patterns inconsistent with normal, individual use. AWS reserves the right to restrict and disable any or all portions of the PSTN Service or Amazon Chime if you or your End Users engage in any prohibited behavior or if necessary for AWS to limit abuse or fraud or to maintain service performance. AWS also reserves the right to modify or remove PSTN telephone number(s) previously assigned to you or your End Users to maintain good quality of service.

70.3. Telephone numbers. If, as a part of Amazon Chime, AWS provides you or your End Users with any telephone number (whether toll or toll-free), you understand and agree that you do not own the number and you do not have the right to keep that number indefinitely. AWS reserves the right to change, cancel or move telephone numbers in its reasonable discretion.

70.4. Other AWS Services. When using Amazon Chime, you and your End Users may also use the Login With Amazon (LWA) Service or other Amazon or AWS Services, and your use of Amazon Chime is subject to the terms that govern those services. You are responsible for separate fees you or your End Users may accrue for using other AWS or affiliated services.

70.5. Log gathering. When you or your End Users use Amazon Chime, we may send one or more cookies that uniquely identifies your browser enabling you to log in faster and enhancing your navigation through Amazon Chime. A cookie may also convey information to us about how you or your End Users use Amazon Chime and allow us to track usage of Amazon Chime over time. For more information on cookies and how to remove them, please consult your specific device's instructions. However, some features of Amazon Chime may not function properly if the ability to accept cookies is disabled. Log file information is automatically reported by your browser or our applications each time you or your End Users access the Service. When you or your End Users use our Service, our servers automatically record certain log file information. These server logs may include anonymous information such as your or your End Users' device data, access data, call statistics, web request, Internet Protocol ("IP") address, browser type, referring / exit pages and URLs, how you interact with the Service, and other such information. We also use your and your End Users' information to send Service-related emails (e.g., account verification, technical and security notices). You and your End Users may not opt out of Service-related e-mails.

70.6. Recording and Retention. You and your End Users have the option to request that Amazon Chime record the applicable audio or video session along with chat and other types of recordings (collectively, "Recording"). If you or your End Users request that an audio or video session or other communications be recorded, Amazon Chime will, in good faith, seek to notify you and your End Users of the Recording by providing a brief audio or visual notice at the time you and your End Users sign in to participate in the applicable session or communication. You and your End Users acknowledge that such notice or attempted notice followed by

the recording of telephone calls and other electronic communications, and that it is your and your End Users' responsibility to comply with all applicable laws regarding the Recording, including properly notifying all participants in a recorded session or to a recorded communication that the session or communication is being recorded and obtain their consent. Neither AWS nor its affiliates will be liable for your or your End Users' unlawful Recording, including failure to provide notice or obtain consent. Any notice provided by AWS to alert participants that a session or communications is being recorded may not be relied upon by you or your End Users as definitive disclosure for your or your End Users compliance with applicable laws regarding the Recording. Further, if you or your End Users use the Service to "chat" with other users of the Service, AWS may retain these chat logs or Recordings for Service-related purposes, or as necessary to comply with the law or a binding order of a governmental body.

70.7. Service Tiers. Unless stated otherwise, your or your End Users' subscription to any of Amazon Chime's free services does not require the payment of a subscription fee. For the avoidance of doubt, your or your End Users' right and license to access, use, execute and deploy any of Amazon Chime's free services are not guaranteed for any period of time, and AWS may restrict, change, limit, or terminate the use of "free" or "basic" versions of Amazon Chime by any individual, entity, or group of entities. If you or your End Users sign up and use a paid version (i.e. Pro) of Amazon Chime and then for any reason, including but not limited to non-payment or breach, your or your End Users' access to the paid services is terminated, you and your End Users may be reverted to the free tier of the Service and may no longer have access to data and other material that you or your End Users may have stored in connection with Amazon Chime and that data and material may be deleted by AWS.

70.8. Emergency Calling. Amazon Chime, including Voice Connector features and Business Calling features, is not a traditional telephone service or a replacement for traditional telephone service. There are important differences between traditional telephone services and Amazon Chime, including Amazon Chime does not support or carry emergency calling to any emergency services personnel or public safety answering points ("Emergency Services") such as 911. You and your End Users understand and agree that it is your responsibility to (i) make alternative arrangements for you and your End Users using Amazon Chime, including Voice Connector features and Business Calling features, to access Emergency Services and (ii) inform all End Users that may use Amazon Chime, including Voice Connector features and Business Calling features, of these limitations and how they may access Emergency Services via other means, including the alternative arrangements that you have made available. Neither AWS nor its affiliates are liable for any damages resulting from any Emergency Services call or any inability to place or complete an Emergency Services call utilizing Amazon Chime, including Voice Connector features and Business Calling features. You agree to indemnify and hold AWS harmless for any claims related to your or your End Users' accounts referring or relating to any Emergency Services call or any inability to place or complete an Emergency Services call utilizing Amazon Chime, including Voice Connector features and Business Calling features.

71. Amazon Connect

71.1. PSTN Service.

Amazon Connect. PSTN Service includes dial-in access to Amazon Connect from the PSTN via standard toll numbers and toll-free numbers.

(b) PSTN Service is sold and provided by AMCS LLC ("AMCS") and not AWS, but is otherwise subject to the terms of the Agreement. Your invoice will clearly state which services that you have used are sold to you by AMCS and which are sold by AWS. The invoicing for PSTN Service is performed by AWS on behalf of AMCS for administrative convenience. You do not have to purchase any AMCS services or PSTN Service to use Amazon Connect, and you may purchase PSTN Service calling features (such as inbound or outbound calling) separately, together or not at all from AMCS. For the avoidance of doubt, AWS is not itself a telecommunications provider and does not itself provide any telecommunications-related services.

(c) Your use of Amazon Connect must comply in all respects with the AWS Acceptable Use Policy. Without limiting the generality of the forgoing, by using the PSTN Service, you acknowledge and agree that the following behavior is prohibited: (i) using PSTN Service in any manner that may expose AMCS, its affiliates, or their personnel to criminal or civil liability; (ii) making calls for purposes that may be considered abusive, fraudulent or unlawful; (iii) resale of the PSTN Service; (iv) calling PSTN telephone numbers (whether singly, sequentially or automatically) to generate income for you or others as a result of placing the call, other than for your or your End Users' individual business communications; or (v) unusual calling patterns inconsistent with normal, individual use. AMCS reserves the right to restrict and disable inbound or outbound PSTN calling if you or your End Users engage in any prohibited behavior or if necessary for AMCS to limit abuse or fraud or to maintain service performance. AMCS also reserves the right to modify or remove PSTN calling inbound calling number(s) previously assigned to you or your End Users to maintain good quality of service.

(d) If as a part of the Amazon Connect service, AMCS provides you with an inbound calling number (whether toll-free or other), you understand and agree that you do not own the number and you do not have the right to keep that number indefinitely. AMCS reserves the right to change, cancel or move telephone numbers in its reasonable discretion.

71.2. No Access to Emergency Services. Amazon Connect is not a replacement for traditional telephone services. There are important differences between traditional telephone services and Amazon Connect. Amazon Connect does not support or carry emergency calling to any emergency services personnel or public safety answering points ("Emergency Services") such as 911 and cannot determine the physical location of call agents and other End Users. You understand and agree that it is your responsibility to (i) make alternative arrangements for you, your call agents and your other End Users that may use Amazon Connect to access Emergency Services and (ii) inform all call agents and other End Users that may use Amazon Connect of these limitations and how they may access Emergency Services via other means, including the alternative arrangements that you have made available. Neither AWS nor its affiliates will be liable for any damages resulting from any Emergency Services call or any inability to place an Emergency Services call utilizing Amazon Connect. You agree to indemnify and hold AWS and its affiliates harmless for any claims referring or

71.3. Service Limitations. There are important service limitations with Amazon Connect. You must carefully review and comply with the applicable Documentation at all times, including limitations related to call rates and frequency, automated calling, calls to certain regions and others. If you believe you will exceed any limitations for legitimate reasons, you must contact customer service ahead of time to request applicable exceptions, which we may or may not make in our sole discretion. Amazon Connect does not support calls to or from facsimile machines or modems. Any caller identification service provided as a part of Amazon Connect is not guaranteed to function at all times.

71.4. Regulatory Compliance. It is your responsibility to use Amazon Connect in compliance with the laws and regulations of the countries where you and your call agents are located, including any regulations governing the use of the Internet for voice communications and messaging. In India, you agree that you will not allow your call agents or other End Users located in India to use Amazon Connect to place calls to Indian telephone numbers or otherwise to third parties located in India. AWS may suspend your use of Amazon Connect for noncompliance with such laws and regulations.

71.5. Recording and Retention. You and your End Users have the option to request that Amazon Connect record an applicable audio session along with chat and other types of recordings (collectively, "Recording"). You and your End Users understand that the making of or use of any Recording may be subject to laws or regulations regarding the recording of telephone calls and other electronic communications or of communications generally, and that it is your and your End Users' responsibility to comply with all applicable laws regarding any Recording, including properly notifying all participants in a recorded session or to a recorded communication that the session or communication is being recorded and obtain their consent. Neither AWS nor its affiliates will be liable for your or your End Users' unlawful Recording, including failure to provide notice or obtain consent. Further, if you or your End Users use the Service to "chat" with other users of the Service, AWS may retain these chat logs or Recordings for Service-related purposes, or as necessary to comply with the law or a binding order of a governmental body.

72. AWS Greengrass

72.1. You are responsible for all applicable fees associated with use of the Services in connection with AWS Greengrass Core. Your use of the AWS Greengrass Core is governed by the AWS Greengrass Core License, located here. AWS Greengrass Core enabled devices must comport with AWS IoT Developer Guidelines and this Agreement.

73. AWS Migration Hub

73.1. AWS Migration Hub requires use of AWS Application Discovery Service ("ADS"), and may include use of AWS Server Migration Service ("SMS") and AWS Database Migration Service ("DMS"). All terms that apply to ADS, SMS, and DMS, including the AWS Connector terms, also apply to your use of AWS Migration Hub.

interfaces with AWS Migration Hub, including Your Content from ADS, SMS, and DMS, will be transmitted to and stored in the AWS Migration Hub region you selected.

73.3. You represent that you have the right to collect and provide the data collected by AWS Migration Hub and its components, including ADS, SMS, and DMS, as applicable ("Hub Information"), and you consent to AWS's collection and provision of Hub Information and the transmission to AWS and processing and use by AWS of the Hub Information in connection with the Service Offerings. Hub Information includes information about your software packages; system, equipment, and application configuration, processes and performance; network configurations, communications and dependencies; relationships between the foregoing; and information about the installation and operation of the AWS Migration Hub and its components.

73.4. You are responsible for determining compliance and complying with the terms of any third party software you use, including any software that interfaces with AWS Migration Hub and its associated software and components, in connection with your use of AWS Migration Hub.

74. Amazon Macie

74.1. You agree that Amazon Macie may use and store Your Content that is processed by Amazon Macie ("Macie Content") to maintain and provide the services (Including but not limited to development and improvement of Amazon Macie) and to develop and improve AWS and affiliate machine-learning and artificial-intelligence technologies.

74.2. While Amazon Macie facilitates the identification of security issues, we do not represent, warrant, or guarantee that all security issues will be identified or that your resources evaluated using Amazon Macie or findings by Amazon Macie, or resources altered based on alerts by Amazon Macie, will be of a certain fidelity, error free, or comply with a particular security standard.

74.3. You are responsible for providing legally adequate privacy notices to End Users of your products or services related to information processed by Amazon Macie and obtaining any necessary consent from such End Users for the processing of Macie Content and the storage and use of Macie Content as described under Section 74.1. You represent to us that you have provided any necessary privacy notices and obtained any necessary consents. You are responsible for notifying us in the event that any Macie Content stored by Amazon Macie must be deleted under applicable law.

75. Amazon MQ (AMQ)

75.1. You acknowledge that neither we nor our licensors are responsible in any manner, and you are solely responsible, for the proper configuration of Amazon MQ including managing the third party message broker settings that are specific to your applications. We may terminate your Amazon MQ instance if you attempt to access or tamper with any software we pre-load on the Amazon MQ instance, including the operating system software running on the Amazon MQ instance.

reasons outside of our control and there is no warranty that the service or content will be uninterrupted, secure or error free or that messages will reach their intended destination during any stated time-frame. Your payment obligations may continue regardless of whether delivery of your messages is prevented, delayed or blocked.

76. AWS Media Services

76.1. The distribution of files created by AWS Media Services may require that you obtain license rights from third parties, including owners or licensors of certain third party audio and video formats. You are solely responsible for obtaining such licenses and paying any necessary royalties or fees.

76.2. We do not represent, warrant or guarantee the quality of any files you create through your use of AWS Media Services or that the files will be of a certain fidelity or error free.

77. Alexa for Business

77.1. "Alexa for Business" means the Alexa for Business Service Offering as described in the Documentation.

77.2. You agree and instruct that: (a) we may use and store Your Content that is processed by Alexa for Business ("Alexa Content") to maintain and provide Alexa for Business (including by not limited to development and improvement of Alexa for Business) and to develop and improve AWS and affiliate machine-learning and artificial intelligence technologies; and (b) solely in connection with the usage and storage described in clause (a), we may store your Alexa Content in AWS regions outside the AWS regions where you are using Alexa for Business.

77.3. The hardware and equipment you use with Alexa for Business must comply with the Documentation provided by AWS. If you use an Amazon device with Alexa for Business, you are subject to and hereby agree to the Amazon Device Terms of Use, except your use of Alexa voice services is subject to the terms of the Agreement. You are responsible for protecting your Alexa for Business devices, including using physical and logical security, firewalls, and other network security tools as appropriate.

77.4. Alexa for Business may include services or applications provided by a third party. Those third party services constitute "Third Party Content" under the Agreement. If you utilize third party services with Alexa for Business, you agree that we may exchange related information with that third party service. Examples of such data include, but are not limited to, device zip code when users ask for the weather, your room names, your room attributes, or the content of your or your End Users' requests. Your or your End Users' use of any third party service is subject to the Agreement and any third party terms applicable to such third party service. Certain of these third party terms may be found in the Amazon Alexa App or may be linked from the Alexa Skills store, and may be updated from time to time. If you do not accept the third party terms applicable to a third party service, do not use that third party service. When using a third party service, you are responsible for any information you or your End Users provide to the third party and adhering to the terms of

77.5. We do not guarantee that Alexa for Business, its functionality, or its content (including traffic, health, or stock information) are accurate, reliable, always available, or complete. Alexa for Business may allow you or your End Users to interact with or operate other products, such as lights, appliances, or video conferencing equipment, and AWS has no responsibility or liability for such products. You or your End Users may encounter content through Alexa for Business that you find offensive, indecent, or objectionable. AWS has no responsibility or liability for such content.

77.6. You are responsible for providing legally adequate privacy notices to your End Users that use Alexa for Business and obtaining any necessary consent from such End Users for the processing of Alexa Content and the storage, use, and transfer of Alexa Content. You represent to us that you have provided any necessary privacy notices and obtained any necessary consents. You are responsible for deleting any Alexa Content stored by Alexa for Business to the extent required under applicable law.

77.7. Alexa for Business is not intended for use in, or in associate with, the operation of any hazardous environments or critical systems that may lead to serious bodily injury or death or cause environmental or property damage, and you are solely responsible for liability that may arise in association with such use.

77.8. You may not market, advertise, or direct Alexa for Business towards anyone under the age of 17.

77.9. Alexa for Business is only available in countries we designate. We may restrict access to Alexa for Business from other locations. AWS is not responsible for any use of Alexa for Business in countries where Alexa for Business is not offered.

77.10. AMCS LLC ("AMCS"), an affiliate of AWS, may offer you certain Alexa-related communication services, such as the ability to send and receive messages, calls, and connect with other users (collectively, "Alexa Calling and Messaging"). Your use of Alexa Calling and Messaging is also subject to the AWS Acceptable Use Policy and Alexa Calling and Messaging Usage Guidelines, which are part of these terms. AMCS and its affiliates may offer services other than Alexa Calling and Messaging, which are not covered by these terms and may be subject to other terms. You, your End Users, or other call participants may be able to ask Alexa for Business to help with certain functions during a call, such as “Alexa, volume up” and “Alexa, hang up.” Certain Alexa Calling and Messaging services are provided by our third party service providers, and we may provide them with information, such as telephone numbers, to provide those services.

77.11. Alexa Calling and Messaging are not a replacement for traditional two-way telephone or mobile phone service, and do not function as such. You acknowledge that Alexa Calling and Messaging do not support or carry emergency calling to any emergency services personnel or public safety answering points (“Emergency Services”), such as 911, and cannot determine the physical location of your devices or your End Users. Alexa Calling and Messaging are not designed or intended to be used to send or receive emergency communications to any police, fire department, hospital, or any other service that connects a user to a public safety answering point. You should ensure you can contact your relevant emergency services providers through a mobile, landline telephone, or other service acceptable to your local 911 provider. You understand and agree that it is your responsibility to: (a) make alternative arrangements for you and your End Users that may use Alexa

other means, including the alternative arrangements that you have made available. Neither AWS nor its affiliates will be liable for any damages resulting from any Emergency Services call or any inability to place an Emergency Services call utilizing Alexa Calling and Messaging and Alexa for Business. You agree to indemnify and hold AWS and its affiliates harmless for any claims referring or relating to any Emergency Services call or any inability to place an Emergency Services call utilizing Alexa Calling and Messaging and Alexa for Business.

77.12. AMCS does not currently charge fees for Alexa Calling and Messaging, but reserves the right to place limitations on use of certain services or features, including subscription or other fees. You and/or the recipient of your or your End Users' calls or messages may be required to pay carrier fees for data usage. AMCS has no responsibility for such fees.

78. Amazon GuardDuty

78.1. Amazon GuardDuty enables you to direct us to generate findings based on third-party threat intelligence provided by you. You are responsible for maintaining licenses and adhering to the license terms of any third-party threat intelligence you provide to generate findings.

78.2. While Amazon GuardDuty facilitates the identification of security issues, we do not represent, warrant, or guarantee that all security issues will be identified or that your resources evaluated using Amazon GuardDuty, or altered based on findings generated by Amazon GuardDuty, will be of a certain fidelity, error free, or comply with a particular security standard.

79. Amazon SageMaker

79.1. You are responsible for providing legally adequate privacy notices to End Users of your products or services that use Amazon SageMaker (including, without limitation, End Users in your private workforce when using Amazon SageMaker Ground Truth) and obtaining all necessary consents from such End Users. You represent to us that you have provided all necessary privacy notices and obtained all necessary consents.

79.2. In conjunction with your use of Amazon SageMaker, you and your End Users may be allowed to use NVIDIA Corporation's CUDA Toolkit or cuDNN software. You agree to be bound by the NVIDIA Cloud End User License Agreement located at https://s3.amazonaws.com/EULA/Nvidia-EULA.txt and NVIDIA third-party materials notices located at https://s3.amazonaws.com/EULA/Nvidia-3P-Notice.txt.

79.3. Amazon SageMaker is not intended for use in, or in association with, the operation of any hazardous environments or critical systems that may lead to serious body injury or death or cause environmental or property damage, and you are solely responsible for liability that may arise in connection with any such use.

79.4. When using the public workforce of Amazon SageMaker Ground Truth: (a) you may not provide datasets that contain protected health information, personal data, or personally identifying information, (b) you may not provide datasets that contain adult content without marking it as containing adult content, and (c) you

80. AWS Single Sign-On (AWS SSO)

80.1. You are responsible for compliance with all end-user agreements and policies for the services or applications you access using AWS Single Sign-On.

81. AWS AppSync

81.1. You may use AWS AppSync to publish, maintain, and monitor Your Content and to accept and process API calls as further described in the Documentation for AWS AppSync.

81.2. By using AWS AppSync you acknowledge and agree that throttling thresholds established by us may vary and cache services may be limited by us from time to time as needed to operate and maintain the AWS AppSync service. In addition and without limiting your obligations under the Agreement, you agree not to and that you will not to attempt to: (i) access any resources not assigned to you by us; or (ii) perform any network discovery or load testing of Your Content inside AWS AppSync unless expressly authorized by us in writing.

81.3. You are responsible for all fees incurred for AWS services that you use in connection with AWS AppSync. You are responsible for the creation, distribution, and security (including enabling of access on any device) of any applications built on AWS AppSync on your AWS account.

82. AWS IoT 1-Click

82.1. The hardware and equipment you use with AWS IoT 1-Click must comply with the Documentation. You are responsible for securing your hardware and equipment, including using physical and logical security, firewalls, and other network security tools as appropriate. You are responsible for applicable fees associated with your use of Services used in connection with AWS IoT 1-Click.

83. General Data Protection Regulation (GDPR)

83.1. These Service Terms incorporate the AWS Data Processing Addendum ("DPA"), available here, when the GDPR applies to your use of the AWS Services to process Customer Data (as defined in the DPA).

83.2. The DPA is effective as of 25 May 2018 and replaces and supersedes any previously agreed data processing addendum between you and AWS relating to the Directive 95/46/EC.

84. Amazon Sumerian

84.1. Sumerian Materials. Amazon Sumerian consists of an integrated development environment and related assets and tools we make available at https://console.aws.amazon.com/sumerian/home (collectively, "Sumerian Materials"). Sumerian Materials are listed in the asset library and may include Sumerian binary files (e.g., images, 3D meshes, and sounds); scripts; text files; hosts (which combine 3D mesh, textures and an

does not include Your Content and/or Content distributed with the Sumerian Materials under separate license terms (such as code licensed under an open source license).

84.2. License. In addition to the rights granted to AWS Content under the Agreement, subject to the terms in the Agreement and in this Section 84, we also grant you a limited, revocable, non-exclusive, non-sublicensable (except to End Users as provided below), non-transferrable license to do the following during the Term:

(a) Development: You may use, reproduce, modify, and create derivative works of the Sumerian Materials to develop and support 3D, augmented reality ("AR") and virtual reality ("VR") applications that run on AR- or VR-enabled (or compatible) platforms, mobile devices and web browsers (each such work, a "Sumerian Scene").

(b) Distribution to End Users: You may use, reproduce, modify, create derivative works of, publicly display, publicly perform, and distribute (including via third party distributors as long as such distribution is done through the applicable Sumerian Scenes' published URL) to End Users the Sumerian Materials (including any permitted modifications and derivatives) as part of a Sumerian Scene. You may sublicense the rights set forth in this Section 84.2, subject to the limitations and restrictions in these terms, to your End Users solely for the purpose of enabling your End Users to use and modify your Sumerian Scene.

(c) Each Sumerian Scene must provide material content or functionality beyond that provided by the Sumerian Materials, and the Sumerian Materials must be integrated into each Sumerian Scene such that they are not separately usable by End Users.

(d) Other Restrictions. Your use of the Sumerian Materials must comply with the Agreement and the AWS Acceptable Use Policy. Without limiting the license restrictions set out in the Agreement, you may not (i) use the Sumerian Materials or any portion thereof as part of a logo or trademark, (ii) remove, obscure, or alter any proprietary rights notices (including copyright and trademark notices) contained in the Sumerian Materials, or (iii) sell, lease, rent or otherwise sublicense or exploit for monetary compensation the Sumerian Materials or any portion thereof, except as part of a Sumerian Scene.

84.3. No License Fee. There is no fee for the licenses granted in Section 84.2. Other fees and terms may apply to Service Offerings and Third Party Content made available in connection with the Sumerian Materials.

85. AWS RoboMaker

85.1. RoboMaker Materials. AWS RoboMaker includes an integrated development and simulation environment and related assets and tools we make available at https://aws.amazon.com/robomaker/ (collectively, "RoboMaker Materials"). RoboMaker Materials are available for download through the AWS RoboMaker Service and may include AWS RoboMaker binary files (e.g., images, 3D meshes, and sounds); scripts; text files; SDF formatted worlds; and basic 3D shapes, such as furniture, lighting and other common objects. RoboMaker Materials are AWS Content under the Agreement.

sublicensable (except to End Users as provided below), non-transferrable license to do the following during the Term:

(a) Development: You may use, reproduce, modify, and create derivative works of the RoboMaker Materials to develop and support AWS RoboMaker test and simulation environments that run on your AWS or on-premises computing resources (each such simulation environment, a "RoboMaker Simulation").

(b) Distribution to End Users: You may use, reproduce, modify, create derivative works of, publicly display, publicly perform, and distribute to End Users the RoboMaker Materials (including any permitted modifications and derivatives) as part of a RoboMaker Simulation. You may sublicense the rights set forth in this Section 85.2 to your End Users solely for the purpose of enabling your End Users to use and modify your RoboMaker Simulation.

(c) Other Restrictions: Each RoboMaker Simulation must provide material content or functionality beyond that provided by the RoboMaker Materials, and the RoboMaker Materials may not be distributed to End Users except as part of a RoboMaker Simulation as permitted by this Section 85.2.

86. Amazon FSx

86.1. Using Microsoft Software. In conjunction with your use of Amazon FSx for Windows File Server, you may use certain software (including related documentation) developed and owned by Microsoft Corporation or its licensors (collectively, the "Microsoft Software"). If you use the Microsoft Software, Microsoft and its licensors require that you agree to these additional terms and conditions:

• The Microsoft Software is neither sold nor distributed to you and you may use it solely in conjunction with the Services.

• You may not transfer or use the Microsoft Software outside the Services.

• You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Software.

• You may not reverse engineer, decompile or disassemble the Microsoft Software, except to the extent expressly permitted by applicable law.

• Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Services.

• Microsoft is not responsible for providing any support in connection with the Services. Do not contact Microsoft for support.

equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, "High Risk Use"). Microsoft and its suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilization of the Microsoft Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.

• Microsoft is an intended third-party beneficiary of these additional terms and conditions, with the right to enforce its provisions.

87. AWS Security Assurance Services

87.1. "AWS Security Assurance Services" are advisory and consulting services that assist you in running regulated data workloads using the Services. AWS Security Assurance Services are provided by AWS Security Assurance Services LLC ("SAS") or certain of its affiliates. SAS is an affiliate of AWS. If SAS provides AWS Security Assurance Services to you, then this Section 87 will apply. References to "Services" in the Agreement include AWS Security Assurances Services.

87.2. To receive AWS Security Assurances Services, you must enter into a statement of work for each specific project that describes the project and additional terms and conditions applicable to the project (each statement of work, a "SOW"). Each SOW is made part of the Agreement. SAS or certain of its affiliates may enter into SOWs with you. For the purposes of a SOW, references to "SAS" in the SOW and references to "AWS" or "SAS" in the Agreement mean references to the SAS entity that enters into the SOW. No SAS entity other than the SAS entity that enters into the SOW has any obligations under such SOW. Any SOW (together with the Agreement as amended by such SOW) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement and supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to such subject matter. If there is a conflict between a SOW and this Section 87, and the SOW explicitly states that it intends to modify the conflicting terms, then the SOW will control.

87.3. Each SOW will show the charges for the AWS Security Assurances Services that SAS will provide. Charges are exclusive of applicable taxes, duties and levies (e.g., VAT, GST, sales tax and use tax). Charges for AWS Security Assurances Services are in addition to any applicable fees for your use of the other Services. SAS, or one of its affiliates on behalf of SAS, will invoice you monthly for the AWS Security Assurances Services and you must pay all invoiced amounts in accordance with the terms of the Agreement. Payments for AWS Security Assurances Services are not refundable.

87.4. You acknowledge that SAS does not provide legal advice. You are responsible for making your own assessment of your legal and regulatory requirements and whether your use of the Services meets those requirements.

provides as part of the AWS Security Assurance Services is "AWS Content." You are solely responsible for testing, deploying, maintaining and supporting Content provided or recommended by SAS.

87.6. Any materials or information that you own or license from a third party that is provided to SAS for the purposes of the AWS Security Assurance Services are "Your Content." If you choose to provide access to Your Content to SAS, then you will ensure that you have adequate rights and permissions to do so.

88. Amazon WorkLink

88.1. You and your End Users may only use the Amazon WorkLink client software on devices owned or controlled by you or your End Users and solely to access Your Content for internal business purposes. You must create an end user account for each End User authorized to access Amazon WorkLink, and each End User may be permitted to use a limited number of devices or sessions in any calendar month. Please see the Documentation for details on creation of End User accounts, and on device or session limits.

88.2. As part of regular operations, Amazon WorkLink may perform configurations, health checks, and diagnostics on a regular basis. To complete these tasks, Amazon WorkLink may access your End Users' devices that are provisioned as part of the Amazon WorkLink setup. During the performance of these tasks, Amazon WorkLink will only retrieve performance, log data, and other information related to the operation and management of the Service.

88.3. You are responsible for providing legally adequate privacy notices to your End Users that use Amazon WorkLink and obtaining any necessary consent from such End Users related to their use of Amazon WorkLink (including the activities described in section 88.2. above). You represent to us that you have provided any necessary privacy notices and obtained any necessary consents. You are responsible for deleting any data generated by Amazon WorkLink and stored by you to the extent required under applicable law.

89. AWS Training and AWS Certification

89.1. AWS Training ("Training") includes instructor led or self-paced digital classes, labs or other training sessions. AWS Certification is a designation certified by AWS on successful completion of role-based or specialty exams that are provided by AWS or an authorized third-party provider. If AWS provides you with either AWS Certification or Training, then this Section 89 will apply. References to "Services" in the Agreement include AWS Certification and Training.

89.2. To arrange on-site instructor led Training for your employees or other individuals (your "Students"), you and AWS or an AWS affiliate must agree to an order form that will provide the details and applicable terms and conditions for your Training. ("Training Order"). Each Training Order will be made a part of the Agreement, and will be the final expression of the terms of the parties' agreement and supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to such subject matter. References to "AWS" in the Training Order mean the AWS entity that executes it, and no other AWS

89.3. For Students whose participation in AWS Training Services has been arranged by a third party (such as the Student's employer or educational institution) ("Coordinator"), AWS will disclose information about the Student's participation to the Coordinator. This information will include a record of the Student's attendance, the results of any test or examination, responses to surveys, and personal data such as the name and the email address used to register for the Training, (collectively "Training Data"). AWS will process personal Training Data in accordance with the AWS Privacy Notice, available at https://aws.amazon.com/privacy. AWS will disclose the Training Data to the Coordinator for certain legitimate business purposes including to (a) confirm that AWS has delivered the Training in accordance with the terms agreed between AWS and the Coordinator, (b) confirm whether the Student has successfully undertaken the Training, and (c) identify additional Training that might be of interest to the Student or the Coordinator.

89.4. Either you or AWS may cancel any on-site Training at least 14 days prior to the start date. If your on-site Training is canceled according to the prior sentence, AWS will refund the cost of that Training class, or reschedule that class on a mutually agreeable date.

89.5. AWS may suspend your access to and use of Training at any time without notice (except as may be prohibited by applicable law) if AWS determines that your or your Students' use of Training violates the AWS Acceptable Use Policy.

89.6. Additional terms and conditions apply to Training in certain jurisdictions. These terms and conditions are available at https://aws.amazon.com/training/jurisdictional-terms/ and are incorporated by reference into the Agreement.

What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal
UK Modern Slavery Statement

Solutions

Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS

SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account
Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon is an Equal Opportunity Employer – Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Tiếng Việt | Türkçe | Русский | ไทย | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy

AWS Shield Advanced Service Level Agreement

Last Updated: March 6, 2019

This AWS Shield Advanced Service Level Agreement ("SLA") is a policy governing your subscription to AWS Shield Advanced under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. and its affiliates ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account subscribed to AWS Shield Advanced. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to prevent AWS resources designated by you for protection by AWS Shield Advanced (the "Designated Resources") from failing to meet any service commitments specified in their respective Service Level Agreements as a result of any denial-of-service attack covered by AWS Shield Advanced (the "Service Commitment"). In the event AWS Shield Advanced does not meet the Service Commitment, you will be eligible to receive a Service Credit. For Designated Resources, a denial-of-service attack covered by AWS Shield Advanced will not constitute an SLA exclusion with respect to a failure to meet any service commitments specified in the relevant SLA.

Service Credits

For each 24-hour interval (Coordinated Universal Time) in which any of the Designated Resources experienced an availability interruption that contributed to AWS Shield Advanced not meeting the Service Commitment, you are entitled to a "Service Credit" in an amount equal to the average daily charges for AWS Shield Advanced for the monthly billing cycle in which the Service Commitment failure occurred. If five or more availability interruptions occur over distinct 24-hour intervals and within a single monthly billing cycle, you are entitled to a Service Credit in an amount equal to 100% of AWS Shield Advanced charges for the monthly billing cycle in which the Service Commitment failures occurred. We will apply any Service Credits only against future AWS Shield Advanced payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service Commitment failure occurred. Service Credits will not entitle you to any refund or other payment from AWS. Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement

a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

(i) the words "SLA Credit Request" in the subject line;

(ii) the dates and times of each incident of availability interruption that you are claiming; and

(iii) your request logs that document the errors and corroborate your claimed availability interruption (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the failure to meet the Service Commitment is confirmed by us, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Prior Version(s): Link

Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal
UK Modern Slavery Statement

Solutions

Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools

Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account

Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon is an Equal Opportunity Employer – Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Tiếng Việt | Türkçe | Русский | ไทย | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy