Contract #: AR3092

STATE OF UTAH COOPERATIVE CONTRACT

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

CodeLynx, Inc.
Name

CodeLynx, Inc. 4937 Fargo Street North
Street Address

Charleston	SC	29418
City	*State*	*Zip*

Vendor # VC226514 Commodity Code #: 920-05 Legal Status of Contractor: Corporation

Contact *Name:* Darren Cumbie *Phone Number:* 855-305-4852 *Email:* Darren.cumbie@codelynx.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: Friday, March 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, etc.

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

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

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

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

CONTRACTOR

Elizabeth W. Heatley 3-1-2019
Contractor's signature Date

Elizabeth W. Heatley
Type or Print Name and Title

DIVISION OF PURCHASING

Chris W Hughes (Mar 14, 2019) Mar 14, 2019
Director, Division of Purchasing Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

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

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

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

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

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

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

10. Defaults and Remedies

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

(1) Nonperformance of contractual requirements; or

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

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

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

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

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

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

13. Indemnification

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

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

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

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

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

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

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

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

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

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

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

16. Insurance

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

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

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

aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

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

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

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

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

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

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

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

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

19. Ordering

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

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

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

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

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

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

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

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

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

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

20. Participants and Scope

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26. Records Administration and Audit.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Services it acquires from this Master Agreement.

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

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

32. Transition Assistance:

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

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

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

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

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

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

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

within the Participating State.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

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

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

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

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

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

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

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.*

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

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	X	X	X	**Microsoft Azure**: Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

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

2.1 Deployment Models.

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

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

Attachment C - Pricing Discounts and Schedule

Contractor: Codelynx

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: Software as a Service (SaaS)

Description	Discount
SaaS Minimum Discount % * (applies to all OEM's offered within this SaaS model	1.25%
Average SaaS OEM Discount Off	**1.25%**

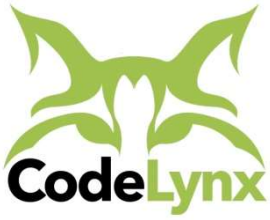
Additional Value Added Services

Item Description	Onsite Hourly Rate NVP Price	Onsite Hourly Rate Catalog Price	Remote Hourly Rate NVP Price	Remote Hourly Rate Catalog Price
Maintenance Services	$ 80.00	$ 85.00	$ 80.00	$ 85.00
Professional Services				
Deployment Services	$ 80.00	$ 85.00	$ 80.00	$ 85.00
Integration Services)	$ 105.00	$ 110.00	$ 105.00	$ 110.00
Consulting/Advisory Services	$ 105.00	$ 110.00	$ 105.00	$ 110.00
Architectural Design Services	$ 130.00	$ 135.00	$ 130.00	$ 135.00
Statement of Work Services	$ 85.00	$ 90.00	$ 85.00	$ 90.00
Partner Services	$ 80.00	$ 85.00	$ 80.00	$ 85.00
Training Deployment Services	$ 76.00	$ 80.00	$ 76.00	$ 80.00
Project Manager	$ 110.00	$ 115.00	$ 110.00	$ 115.00
Network Enginner III	$ 100.00	$ 105.00	$ 100.00	$ 105.00
Software Developer V	$ 120.00	$ 125.00	$ 120.00	$ 125.00
Software Developer IV	$ 95.00	$ 100.00	$ 95.00	$ 100.00

	Deliverable Rates NVP Price	Deliverable Rates Catalog Price
Program Manager	$ 125.00	$ 135.00
Installation Engineer	$ 80.00	$ 85.00
Quality Assurance Analyst III	$ 85.00	$ 90.00
Quality Assurance Analyst II	$ 71.00	$ 75.00
Business Analyst III	$ 80.00	$ 85.00
Business Analyst II	$ 62.00	$ 65.00
Information Assurance III	$ 125.00	$ 130.00
Information Assurance II	$ 105.00	$ 110.00
Information Assurance I	$ 85.00	$ 90.00
Database Administrator II	$ 110.00	$ 115.00
Database Administrator I	$ 85.00	$ 90.00
Senior Software Architect	$ 145.00	$ 150.00

RFP #SK18008
Proposal

4937 Fargo Street
North Charleston SC 29418
Phone 843.266.2330 | Fax 843.266.2333
www.codelynx.com



Utah Solicitation Number SK18008

Technical Response

NASPO ValuePoint Agreement for Cloud Solutions

Prepared on July 6, 2018 by:

Darren Cumbie

Director of Software Development, CodeLynx

Darren.Cumbie@codelynx.com

8 Technical Requirements

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

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

8.1 Technical Requirements

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

Microsoft Azure offers both commercial and government side service models that offer a plethora of cloud services within Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service Models (SaaS).

NIST 800-145 outlines the *Essential Characteristics* of these models as the following: On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Microsoft Azure supports on-demand self-service by enabling the provision of resources on demand whenever required without human interaction. Services can be enabled from Portal (web site), Azure API, or command line interfaces for Linux, Mac, and Windows. Infrastructure scaling of resources is on-demand self-service via programmatic interfaces pre-set within the environment.

Microsoft Azure supports broad network access through their utilization of the Azure Portal for management of resources which is available on mobile phones, tablets, laptops, and workstations. Azure additionally supports VPN connections for devices through standard VPN, ExpressRoute gateway connections and the Azure Virtual Network to connect on-premise networks with networks and virtualized environments in Azure.

Azure implements resource pooling through the utilization of a multi-tenant model where various physical and virtual resources are assigned and/or reassigned according to consumer demand. Azure provides location independence within their datacenters yet provides specification of higher level abstraction of location via the Azure Regions. Allowing clients to know which region or in some cases which state their resources are located within. Though the Customer may not be able to dictate the exact location in a datacenter that their hardware is located, they have a choice as to what type/level and availability of hardware their applications/service/infrastructure is hosted on depending on budget and necessity.

Azure may be modified instantaneously as dictated by requirements. The Azure portal allows for instant allocation of additional resources and instant removal of resources to provide the best value to the end-customer. A virtual machine, WebApp, unit of storage, etc. may be allocated, modified, and removed all in one day while the customer only pays for the usage of those resources during the time that they are reserved and/or active.

Measured service is accomplished through the Azure Portal as well. The intuitive interface allows for quick reference of utilization, periods of high usage, and periods where resource utilization is in a trough. The tools and features contained in the portal allow unutilized resources to be turned off during identified periods of inactivity and allowing the customer to reap the savings benefits through conscious-minded administration.

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

CodeLynx is willing to comply with the requirements of Attachments C & D for each of the three service models SaaS, PaaS, and IaaS that are being offered in this proposal.

CodeLynx will agree, on behalf of Microsoft, that during the term of a Purchasing Entity's subscription for its Azure commercial and Azure Government (as defined in Microsoft's terms and conditions), those services will be operated in accordance with a written data security policy and control framework that is consistent with the requirements of NIST 800-53 Revision 4, or successor standards and guidelines (if any), established to support Federal Risk and Authorization Management Program (FedRAMP) accreditation at a Moderate Impact level.

Additional information regarding Microsoft Azure's compliance may be found on their Trust Center portal (https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings), and include, but are not limited to:

Globally: CSA-STAR, DFARS, ISO 20000-1:2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 9001, SOC (1,2,3), and WCAG 2.0

US: CJIS, DoD DISA (L2, L4, L5), DoE 10 CFR Part 810, EAR (US Export Administration Regulations), FDA CFR Title 21 Part 11, FedRAMP, FERPA, FIPS 140-2, IRS 1075, ITAR, NIST 800-171, NIST Cybersecurity Framework (CSF), and Section 508 VPATS.

Industry Specific: 23 NYCRR 500, CDSA, FFIEC, CLBA, GxP, HIPAA/HITECH, HITRUST, MARS-E, MPAA, PCI DSS, and SOX.

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

CodeLynx has provided the *Services* requirements of *Section 1.1.3* Attachment D: Scope of Services in Response 8.1.1 above. While the remaining requirements are explained below.

Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud "tenants." You access services and manage your account using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

Hybrid cloud models can be achieved through using Azure Stack. Azure Stack enables you to deploy Azure services on-premises or in the cloud with a consistent application logic, development paradigm, and operations methodology.

Hybrid cloud applications are a single system that has components running in both Azure and Azure Stack. This solution blueprint is relevant to establishing connectivity for any application that involves communications between the Azure public cloud and on-premises Azure Stack components. Hybrid connectivity is a foundational blueprint that will be applicable to most Azure Stack solutions.

CodeLynx can provide any of the three Service Models (SaaS, IaaS, and PaaS), separately or in combination within Microsoft Azure. Customers may select the best model that fits their needs and budget to accomplish critical processes while utilizing a cost-effective and highly-available solution.

NIST SP 800-145 defines Software-as-a-Service (SaaS) as "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either 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, except for limited user-specific application configuration settings."

Common examples of SaaS are email, calendars, and productivity tools such as Microsoft Office 365. SaaS requires no need to purchase, install, update, or maintain any hardware, middleware, or software, and allows the organization to pay for only the resources that they utilize.

Each Azure SaaS offering is accessible to client devices through thin client interfaces (web browsers) as is the case of Power BI or program interfaces as is the case with Visual Studio. The consumer does not manage or control the underlying cloud infrastructure.

NIST SP 800-145 defines Platform-as-a-Service (PaaS) as "The capability provided to the consumer is to deploy onto the cloud infrastructure, consumer-created or acquired applications created, using programming languages, libraries, services, and tools supported by the provider. 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 configuration settings for the application-hosting environment."

Each Azure PaaS offering gives the consumer control over the deployed application and configuration settings for the application-hosting environment. An example of these configuration settings would include the ability to set the URL for an App Service Web App instance or to configure the amount of computational power made available to a particular database in an Azure SQL instance. The consumer does not control the underlying cloud infrastructure such as network, servers, operating systems, or storage in a PaaS offering and as such those settings are not exposed in Azure.

NIST SP 800-145 defines Infrastructure-as-a-Service (IaaS) as "The capability provided to the consumer is 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, and deployed applications; and possibly limited control of select networking components."

IaaS allows users the capability of defining the hardware, networking and firewalls, and servers and storage that they utilize all with a few mouse clicks within the Azure Portal. Storage can be allocated. Virtual machines can be powered on, configured, modified, turned off, and deleted. Virtual networks can be set up to improve security posturing. All without having to purchase an additional piece of hardware to see it come to fruition. The organization simply pays for the time and resources consumed while the virtualized environment is in production. The major benefit is the cloud computing service provider manages the infrastructure, while you purchase, install, configure, and manage your own software—operating systems, middleware, and applications.

Managing an IaaS environment provides the most customization that Azure has to offer. As with any deployment choice there are positives and negatives to be weighed. The greatest benefit of an IaaS implementation is that it offers the greatest amount of control by the consumer. However, with more control comes more overhead of maintenance and monitoring.

The IaaS capabilities offered by Azure provide the consumer with the capability to provision processing, storage, networks, load balancers, DNS, along with numerous other resources that allow the consumer to deploy and run arbitrary software. Said software can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has full control of all deployed virtual appliances, networking components, operating systems, storage, and deployed applications.

8.2 Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business, and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

CodeLynx Response:

CodeLynx will be reselling Microsoft products and services directly to customers through the NASPO contract agreement. We will work with each customer to determine the scope of their needs as well as provide quotes, licensing agreements, usage reports, and billing for Microsoft products.

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

CodeLynx Response:

CodeLynx will work directly with all NASPO partners and entities to meet the requirements of this RFP. We will procure, configure, implement, and maintain all Microsoft products and services purchased through this

agreement. CodeLynx can offer Project Management services to our customers to ensure migrations to the cloud and cloud implementations happen efficiently and effectively.

CodeLynx provides support to our customers on all procurement, configuration, implementation, maintenance, usage, and billing needs. For support related directly to Microsoft products and services, CodeLynx can direct customers to the appropriate contact or initiate support through our service agreement and partnership with Microsoft.

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

CodeLynx Response:

As mentioned throughout this document CodeLynx will utilize Microsoft as the subcontractor for all the services mentioned in this response. Microsoft is an industry leader in the commercial and government cloud market. Microsoft does not accept flow-down of Statement of Work requirements.

8.3 Working with Purchasing Entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;

Response times;

Processes and timelines;

Methods of communication and assistance; and

Other information vital to understanding the service you provide.

CodeLynx Response:

Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;

The CodeLynx Contract Manager will report the incident to designated customer's Information Owner and/or Information Systems Security Manager. Both CodeLynx Information Owner and Information Systems Security Managers will work in conjunction with Microsoft's Security team through the Identification, Containment and Eradication phases of a breach and/or confirmed incident.

Response times;

Microsoft continuously monitors for information security. Response to incidents start immediately after initial discovery and an Incident Assessment Phase. Notification to customers occurs after an incident is confirmed and constitutes the Customer Notification Phase. During the customer notification phase the Global Administrator for an Azure resource is contacted. If, due to contract specifications, the Global Administrator is a CodeLynx employee and not a client employee, CodeLynx will immediately reach out to the client for notification.

Processes and timelines;

CodeLynx Inc. will provide breach notification during the Customer Notification phase shown above, approximately seventy-two (72) hours from a confirmed breach discovery in accordance with DFARS 252.204-7012 and GDPR requirements regulations.

Methods of communication and assistance;

Until extent of the breach is confirmed, communications between CodeLynx Inc. and customer will be exclusively through voice communications. Use of email communications is discouraged during the identification phase of the incident.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

CodeLynx acknowledges that it will neither engage nor permit CodeLynx agents/employees to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

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

CodeLynx Response:

Azure supports the creation of test/staging environments that can be created to be identical to production environments. This is accomplished by adding duplicate resources of the production environment to a test/staging resource group or even under a separate subscription maintained strictly for testing or staging items.

8.3.4 Offeror must describe whether its computer applications and Web sites are accessible to people with disabilities and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

Microsoft Azure has achieved the WCAG 2.0 (ISO/IEC 40500) certification by tirelessly working with governments and organizations the world over to provide the benefits of digital technology to people with disabilities. Microsoft is a signatory to the Global Initiative for Inclusive Information and Communications Technology (G3ict). Microsoft does not hold only one certification. They have achieved EN 301 549, and U.S. Section 508 compliance.

8.3.5 Offeror must describe whether its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

Currently, the Azure Portal supports the latest releases of Microsoft Edge, Safari, Chrome, Firefox, and Internet Explorer 11.

(https://docs.microsoft.com/en-us/azure/azure-preview-portal-supported-browsers-devices)

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

When requested, CodeLynx, in conjunction with Microsoft, will coordinate cooperative meetings pertaining to information storage and security. CodeLynx will only store Customer billing information. The Customer's data will be maintained in accordance with Microsoft's privacy conditions found at: https://www.microsoft.com/en-us/trustcenter/privacy

"Microsoft makes broad contractual commitments to business in our Online Services Terms. Microsoft will use customer data only to provide the services agreed upon, and for purposes compatible with providing those services. We do not use customer data or derive information from it for advertising.

Furthermore, we will not disclose customer data hosted in Microsoft business services to a government agency unless required by law. If law enforcement demands customer data, we will attempt to redirect the agency to request that data directly from the customer. If we are compelled to disclose customer data to law enforcement, we promptly notify the customer and provide a copy of the demand, unless legally prohibited from doing so.

In addition, we make specific, contractual, privacy-related commitments." Retrieved from https://www.microsoft.com/en-us/trustcenter/privacy/we-set-and-adhere-to-stringent-standards

Microsoft's SLA's may be found via the following link: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

For ease of obtaining this information, customers can refer to Microsoft's Trust Center to obtain a plethora of information about compliance, security, privacy, and more: https://www.microsoft.com/en-us/trustcenter/compliance/default.aspx

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

CodeLynx Response:

CodeLynx utilizes Agile-Scrum methodologies to plan, implement, and test all work involved with a project. All project schedules depend on well-defined requirements, with clear acceptance criteria to confirm that all features meet client, company, and industry standards. Once all requirements are identified and defined,

CodeLynx will work directly with the customer to produce a timeline that fits their need, but also allows a complete and thorough solution to be in place.

Agile Scrum Methodology

- Capture / Document Requirements (project kickoff meeting, configuration control board meeting)
- Define Requirements
- Estimate PBIs
- Plan (features, modules, releases, customized schedule)
- Work (commit to sprint, develop, DEV/QA/BA testing)
- Deploy (system integration testing, version release, acceptance testing)

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

How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.

CodeLynx Response:

CodeLynx works with existing government contracting agencies to add or update prices and offerings on a continuous basis. As it pertains specifically to the Cloud landscape, the continuing evolution of technologies and hardware will continue to provide economies of scale which will continue to drive pricing down over time. These same advances give rise to new offerings such as Artificial Intelligence in the cloud which creates brand new types of offerings. CodeLynx has worked with federal and state agencies to incorporate these changes from Economic Price Adjustments to implementations of new technologies and how they are impacted by FAR, DFAR, or State level Procurement Codes. Our Contract Manager, legal, accounting and sales teams are familiar with implementing and adopting these changes to ensure that they comply with the requirements of our existing contracts.

How Offeror will maintain discounts at the levels set forth in the contract.

CodeLynx Response:

CodeLynx maintains a quality management program and cost control program to ensure internal costs are kept low for customers and government entities. In addition to the CodeLynx controls, the trends of Cloud and all computing is that costs come down over time through economies of scale. CodeLynx also has the ability to offer greater discounts on various projects depending on size and scale of the particular project and the Cloud requirements.

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

CodeLynx Response: CodeLynx provides updates through regular account manager calls, blog posts, support newsletters, and via in-person meetings and events. CodeLynx takes great pride in embracing new and disruptive technologies. This is particularly true in the Cloud environment. If a change in the way a solution is deployed can drive better performance and user experience, lower costs or both then the CodeLynx team will work to educate the Purchasing Entity of the opportunity. This has been a frequent conversation going from a traditional IaaS deployment to a PaaS deployment where the architectural change leads to a more robust, scalable and usually less costly operating picture. Our various team members work to communicate these types of opportunities to agencies and determine if it is something they are able to take advantage of for their organization.

How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

CodeLynx Response:

CodeLynx works with all our clients to mitigate any impact to operations that a service change will pose. CodeLynx does this first by communicating information about changes as far in advance as possible. Once an impact has been identified the CodeLynx project management and account representatives will work with the purchasing entity and its stakeholders to create a transition plan. From there the teams will hold regular recurring (usually bi-weekly) standing calls to brief needed stakeholders on the status of each task in the transition plan. CodeLynx has also been able to work with customers on a case by case basis in the past to make special exceptions to support them beyond End of Life or End of Support for specific products. Exceptions cannot be made for service changes that deal with security or addressing any known vulnerabilities.

8.4 Customer Service

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

Quality assurance measures;

Escalation plan for addressing problems and/or complaints; and

Service Level Agreement (SLA).

CodeLynx Response:

For each customer engagement, CodeLynx provides an experienced customer support team comprised of the Director of Software Engineering, an Account Executive, a Project Manager, and a Quality Assurance

Engineer, all of which are empowered to make decisions in support of customer needs, requirements, and issue resolution. We are committed to our customers and provide a customer support plan for each engagement that includes current contact information for each member of the customer support team, detailed quality assurance measures, an issue escalation plan, and any SLAs applicable to the engagement.

CodeLynx knows successful projects require clear and frequent communication throughout the project life cycle, as well as hands-on reviews as the project progresses. We use an agile methodology to ensure customers are kept up to date throughout the life of a project. Through frequent reviews, customers are given unique opportunities to provide feedback and guide implementation. This allows us to quickly identify any misunderstandings and adjust our efforts to get the project back on track without disruption to the timeline or budget.

In addition to our customer support team, agile methodology, and proven communication skills, CodeLynx offers extensive quality assurance measures. CodeLynx quality assurance engineers perform complete end-to-end testing to ensure solutions function as required. Quality Assurance engineers adhere to strict testing standards that include quality assurance analysis, automated testing, and acceptance testing. Every feature is tested by the engineers immediately following its implementation. After all features and configurations are implemented, the engineer releases the solution to the quality assurance analyst who will test all functionality. This includes compatibility testing on all required operating systems. In addition to Quality Assurance testing, CodeLynx uses automated testing when applicable. This is an extra level of testing that occurs simultaneously with quality assurance testing to ensure defects and issues within the solution are identified and resolved quickly. After the solution is fully tested by Quality Assurance engineers, CodeLynx presents the solution to the customer for review and acceptance. In the event that issues are found by the customer, CodeLynx will resolve the issues and retest the solution.

Microsoft Response:

For complete details regarding Microsoft Azure Product Service Level Agreements, please visit https://azure.microsoft.com/en-us/support/legal/sla/

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

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

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

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

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

CodeLynx Response:

CodeLynx appoints a specific customer support team to each customer with our Director of Software Engineering acting as the lead representative for each entity that executes a Participating Addendum. Contact information for the director and all customer support team members, including Account Executives and Project Managers, will be provided to all customers, and updated on a regular basis, to ensure this information remains current. CodeLynx is also happy to provide this information to NASPO frequently if needed.

CodeLynx customer service representatives are available by phone or email from 7AM to 6PM Monday through Friday. CodeLynx provides customers with access to representatives Saturday and Sunday, as well as during non-business hours (6 PM – 7AM), for assistance with emergencies and high-priority needs. Customer service and support plans can be customized for each customer to fit specific customer service needs.

It is CodeLynx policy for customer service representatives to respond to inquiries at a minimum within one business day.

Microsoft Response:

In addition to the support CodeLynx can offer customers through our Microsoft Partnership, customers can purchase a Microsoft Azure support plan that would grant direct access to Microsoft customer service representatives if they prefer. Microsoft offers five Azure support plans:

Basic: 24/7 access to customer service, documentation, whitepapers, and support forums applicable to billing and subscription support, as well as online self-help through community forums managed by Microsoft employees and associates. This support plan is offered for free to all Azure customers.

Developer: Response time is less than 8 business hours

Standard: Response time of less than 8 hours for minimal business impact inquires, response time of less than 4 hours for moderate business impact inquires, and response time of less than 1 hour for critical business impact inquires

Professional Direct: Response time of less than 4 hours for minimal business impact inquires, response time of less than 2 hours for moderate business impact inquires, and response time of less than 1 hour for critical business impact inquires

Premier: Same response times as Professional Direct subscriptions with the option to reduce critical business impact inquires to less than 15 minutes with Azure Rapid Response or Azure Event Management.

8.5 Security and Information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Microsoft has leveraged its decades-long experience building enterprise software and running some of the world's largest online services to create a robust set of security technologies and practices. These ensure that Azure infrastructure is resilient to attack, safeguards user access to the Azure environment, and helps keep customer data secure through encrypted communications as well as threat management and mitigation practices, including regular penetration testing.

Managing and controlling identity and user access to your environments, data, and applications by federating user identities to Azure Active Directory and enabling multi-factor authentication for more secure sign-in.

Encrypting communications and operation processes. For data in transit, Azure uses industry-standard transport protocols between user devices and Microsoft datacenters, and within datacenters themselves. For data at rest, Azure offers a wide range of encryption capabilities up to AES-256, giving you the flexibility to choose the solution that best meets your needs.

Securing networks. Azure provides the infrastructure necessary to securely connect virtual machines to one another and to connect on-premises datacenters with Azure VMs. Azure blocks unauthorized traffic to and within Microsoft datacenters, using a variety of technologies. Azure Virtual Network extends your on-premises network to the cloud through site-to-site VPN.

Managing threats. To protect against online threats, Azure offers Microsoft Antimalware for cloud services and virtual machines. Microsoft also employs intrusion detection, denial-of service (DDoS) attack prevention, regular penetration testing, and data analytics and machine learning tools to help mitigate threats to the Azure platform.

CodeLynx has our own policies to safeguard from an order processing and billing perspective. CodeLynx complies with PCI DSS, HIPAA, and Sarbanes-Oxley. For example, encryption is in place to protect Confidential/Restricted information.

Our record retention schedule is enforced based on record type, not by customer. Once the retention period has been reached, the data is deleted from our systems. Should CodeLynx be awarded this RFP, CodeLynx will provide additional details regarding the scope of the disposal processes.

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

CodeLynx complies with PCI DSS, HIPAA, and Sarbanes-Oxley. As it pertains to Microsoft Online Services sold under the Master Agreement, CodeLynx and Microsoft will comply with all applicable laws (including but not limited to privacy and security related laws) applicable to IT service providers. For clarity, however, CodeLynx and Microsoft do not agree to comply with laws written to apply solely to governments and their government functions (or to companies and their industry functions). For example, some laws pertaining to notification of security incidents apply to our government customers (not to IT Service Providers), so CodeLynx and Microsoft do not agree to comply with those (but we believe our contractual commitments for Security Incident reporting are sufficient to help customers comply with their own laws).

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Governed by Microsoft privacy policies and the Microsoft Privacy Standard, privacy is built into the infrastructure of Microsoft cloud services.

The Microsoft Privacy Standard is a cornerstone of the privacy program at Microsoft. This authoritative document describes the Microsoft privacy program, including the business processes we follow to achieve privacy compliance. It also delineates the general privacy rules and requirements for developing and deploying Microsoft products and services, including those in the Microsoft Cloud. It sets rules to help Microsoft keep your customer data secure, and handle and store the data you entrust to them in a way that helps protect its privacy.

Microsoft Security Development Lifecycle (SDL). Privacy requirements are defined and integrated early in the SDL, a software development process that helps developers build Microsoft Cloud services and features that are more secure and that help address data protection and privacy requirements. As part of this process, the SDL is designed to support effective privacy reviews of each release of a Microsoft Cloud service.

Microsoft contractual commitments back their privacy best practices.

Online Services Terms. These are the contractual commitments Microsoft makes to their enterprise cloud customers to secure and protect both the use and the disclosure of customer data. We have included a copy of these terms as an attachment to this response. Microsoft will use customer data only to provide the services agreed upon, and for purposes (such as troubleshooting and protection against malware) compatible with providing those services. They do not use customer data or derive information from it for advertising. Furthermore, they will not disclose customer data hosted in the Microsoft Cloud to government agencies except as you direct or where required by law. If they do receive a request, they will promptly notify you unless legally prohibited from doing so.

ISO/IEC 27018:2014. Microsoft was the first major cloud provider to adopt this first international code of practice for cloud privacy. ISO/IEC 27018 was developed to establish a uniform international approach to protecting the privacy of personal data stored in the cloud by data processors. As part of the certification process for ISO/IEC 27001, accredited certification bodies independently verified that in-scope Microsoft enterprise cloud services have incorporated ISO/IEC 27018 controls. These controls include a prohibition on the use of customer data for advertising and marketing purposes without the customer's express consent. Microsoft contractually commits to complying with ISO/IEC 27018.

EU Model Clauses. EU data protection law regulates the transfer of EU customer personal data to countries outside the European Union. Microsoft offers customers the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services. Europe's privacy regulators have determined that the contractual privacy protections that the Microsoft Cloud delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Microsoft was the first cloud provider to receive this recognition.

8.6 Privacy and Security

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

Microsoft enterprise cloud services are independently validated through certifications and attestations, as well as third-party audits. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, such as ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1 and SOC 2. They also meet regional and country specific standards and contractual commitments, including the EU Model Clauses, UK GCloud, Singapore MTCS, and Australia CCSL (IRAP). In addition, rigorous third-party audits, such as by the British Standards Institution and Deloitte, validate the adherence of our cloud services to the strict requirements these standards mandate. For more information, please refer to the Windows Azure Security Privacy Compliance document included with our Minimum Mandatory response.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Microsoft continually strives to maintain compliance and broaden its compliance spectrum. At the time of drafting this proposal, Microsoft has published that it is compliant with over 60 certifications for Microsoft Azure alone.

Global certifications include CSA-STAR, DFARS, ISO 20000:1:2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 9001, SOC (1,2,3), GDPR, and WCAG 2.0.

U.S. Government certifications include: CJIS, DoD DISA (L2,L4,L5), DoE 10 CFR Part 810, EAR (US Export Administration Regulations), FDA CFR Title 21 Part 11, FedRAMP, FERPA, FIPS 140-2, IRS 1075, ITAR, NIST 800-171, NIST Cybersecurity Framework (CSF), and Section 508 VPATs.

Further, Microsoft maintains industry specific certifications such as: 23 NYCRR 500, CDSA, FFIEC, GLBA, GxP, HIPAA/HITECH, HITRUST, MARS-E, MPAA, PCI DSS, SOX, and more.

The expanded list contains certifications that are applicable only on foreign soil, and applicable certifications are obtained regularly by Microsoft. The updated list can be found at: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

Microsoft Azure offers a variety of mechanisms to secure data and applications based on the Customer's business needs. Security and privacy are built right into the Azure platform, beginning with the Security Development Lifecycle (SDL – see https://www.microsoft.com/en-us/sdl/default.aspx for the detailed Security Development Lifecycle). The SDL addresses security at every development phase and ensures that Azure is continually updated to make it even more secure. Operational Security Assurance (OSA) builds on SDL knowledge and processes to supply a framework that helps provide secure operations throughout the

lifecycle of cloud-based services. Azure Security Center makes Azure the only public cloud platform to offer continuous security-health monitoring.

Azure helps you protect business and personal information by enabling you to manage user identities and credentials plus control access.

Azure Active Directory

Helps ensure that only authorized users can access your environments, data, and applications.

Offers multi-factor authentication for highly secure sign-in, including specialized administrative access through Azure Active Directory Privileged Identity Management.

Performs authentication, authorization, and access control through industry-standard protocols such as SAML 2.0, WS-Federation, and OpenID Connect.

Helps developers integrate identity management into apps across different platforms and build mobile and web apps that integrate with Microsoft and third-party APIs with OAuth 2.0.

Works as a standalone cloud directory for your organization or can be integrated with your on-premises Active Directory with directory sync and single sign-on (SSO).

Allows federated applications to support user provisioning and password vaulting.

Protect data with Azure Multi-Factor Authentication

Requires users to verify their sign-ins via mobile app, phone call, or text message.

Office 365 includes a form of Multi-Factor Authentication.

Azure Active Directory Premium edition adds Multi-Factor Authentication custom greetings, fraud alerts, security reports, one-time bypass, blocking/unblocking of users, customizable caller ID for authentication phone calls, and more.

Azure and data encryption

Azure uses industry-standard protocols to encrypt data in transit. Your data is secure as it travels between devices and Microsoft datacenters, as it moves within datacenters, and when your data is at rest in Azure Storage. Capabilities include:

Protects data in transit and at rest, including encryption for data, files, applications, services, communications, and drives.

Supports and uses numerous encryption mechanisms, including SSL/TLS, IPsec, and AES.

Provides configuration support for BitLocker Drive Encryption on VHDs that contain sensitive information.

Ensures that access to data by Azure support personnel requires your explicit permission and is granted on a “just in time” basis that is logged and audited, then revoked after completion of the engagement.

Azure Key Vault service

Secure key management is essential to protecting data in the cloud. Azure Key Vault enables Azure subscribers to safeguard and control cryptographic keys and other secrets used by cloud apps and services.

Encrypt keys and small secrets like passwords using keys in Hardware Security Modules (HSMs).

Import or generate your keys in HSMs certified to FIPS 140-2 level 2 standards for added assurance so that your keys stay within the HSM boundary.

Simplify and automate tasks for SSL/TLS certificates by enrolling and automatically renewing certificates from supported Public Certification Authorities (CAs).

Provision and deploy new vaults and keys in minutes without waiting for procurement, hardware, or IT and centrally manage keys, secrets, and policies.

Maintain control over encrypted data—grant and revoke key use by your own and third-party applications as needed.

Segregate key management duties so developers can easily manage keys used for dev/test and migrate seamlessly to production keys managed by security operations.

Rapidly scale to meet the cryptographic needs of your cloud applications and match peak demand.

Achieve global redundancy by provisioning vaults in Azure datacenters worldwide and keep a copy in your own Hardware Security Modules (HSMs) for added durability.

Data and storage security features

You can encrypt your data before putting it into Azure and you can store keys in your on-premises datacenter.

Client-side encryption for Azure Blob storage enables you to completely control the keys. The storage service never sees the keys and is incapable of decrypting the data. Azure Storage automatically encrypts your data prior to persisting to storage and decrypts prior to retrieval.

Storage Account Keys, Shared Access Signatures, management certificates, and other keys are unique to each Azure tenant.

You can use Azure Rights Management Services (RMS) for file- and data-level encryption and to prevent unintentional or deliberate leakage of data by authorized users.

Azure Virtual Networks

Provide more secure infrastructure design and controls

The Azure infrastructure is designed as a secure foundation that can host millions of customers simultaneously, giving you control and customization via a wide array of configurable security options. Azure prevents unauthorized and unintentional transfer of information between deployments in a multitenant architecture, using virtual local area network (VLAN) isolation, access control lists (ACLs), load balancers, and IP filters, along with traffic flow policies. Network address translation (NAT) separates internal network traffic from external traffic.

Extend your on-premises network to the cloud via a site-to-site virtual private network (VPN) or a dedicated wide area network (WAN) link.

Use Azure ExpressRoute to create a cross-premises connection.

Provide more secure infrastructure design and controls

The Azure infrastructure is designed as a secure foundation that can host millions of customers simultaneously, giving you control and customization via a wide array of configurable security options. Azure prevents unauthorized and unintentional transfer of information between deployments in a multitenant architecture, using virtual local area network (VLAN) isolation, access control lists (ACLs), load balancers, and IP filters, along with traffic flow policies. Network address translation (NAT) separates internal network traffic from external traffic.

Azure Fabric Controller

Allocates infrastructure resources to tenant workloads and manages unidirectional communications from the host to VMs.

Uses the Azure hypervisor to enforce memory and process separation between VMs and to securely route network traffic to guest OS tenants. Azure also implements isolation for tenants, storage, and virtual networks.

Network Security Groups (NSG)

NSGs allow control of traffic to Virtual Machine (VM) instances.

NSGs, user-defined routing, IP forwarding, forced tunneling, and endpoint ACLs help secure communications on Azure Virtual Networks.

Azure implements packet-filtering firewalls on all host and guest VMs by default.

Physical infrastructure security

Azure is deployed in Microsoft regional datacenters. These datacenters are protected by layers of defense-in-depth security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communication networks. This multi-layered security model is in use throughout every area of the facility, including each physical server unit.

Defend Against Threats

Microsoft continuously monitors servers, networks, and applications to detect threats. The Azure multipronged threat-management approach includes technologies and processes to constantly strengthen Azure's defenses and reduce risks and include:

Intrusion detection

Distributed denial-of-service (DDoS) attack prevention

Penetration testing

Behavioral analytics

Anomaly detection

Machine learning

Microsoft Antimalware for Azure

Protects Azure cloud services and virtual machines.

Supports deployment of third-party security solutions within your subscriptions, such as web application firewalls, network firewalls, antimalware, intrusion detection and prevention systems (IDS/IPS), and more

Azure Security Center

Gives you control over the security of your cloud assets.

Lets you define policies for your Azure subscriptions, deploy integrated security solutions from Microsoft and its partners, and get a centralized view of the security state of all your Azure resources.

Azure Log Integration allows you to integrate these logs from assets deployed in Azure to on-premises security information and event management (SIEM) systems.

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

Both Azure Government and commercial offerings deliver a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft. Below are the key security control areas that Microsoft has invested in.

Infrastructure Protection

Azure infrastructure includes hardware, software, administrative and operations staff, and physical data centers. Azure addresses security risks 24X7 across its infrastructure with continuous intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools that help identify and mitigate threats. With Azure, customers can reduce the need to invest in these capabilities on their own and benefit from economies of scale in Microsoft datacenter infrastructure.

§ **24 hour monitored physical security** - Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

§ **Monitoring and logging** - Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts.

§ **Patching** - Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.

§ **Antivirus/Antimalware protection** - Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software

and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.

§ **Intrusion detection and DDoS** - Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.

§ **Penetration testing** - Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of a customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their applications hosted in Azure.

Network Protection Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Azure blocks unauthorized traffic to and within Microsoft data centers using a variety of technologies such as firewalls, partitioned Local Area Networks, and physical separation of back-end servers from public-facing interfaces.

Virtual networking. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other using private IP addresses. Each virtual network is isolated from other virtual networks.

§ **Encrypting communications**. Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on premise data centers. Encryption can be configured to protect administrator access to virtual machines through remote desktop sessions and remote Windows PowerShell. Access to the Azure Management Portal is encrypted by default using HTTPS. Identity and Access Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications.

Identity and Access

Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications.

§ **Access monitoring and logging** - Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.

§ **Strong authentication** - Azure Multi-Factor Authentication reduces organizational risk and helps enable regulatory compliance by providing an extra layer of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. Azure Multi-Factor Authentication can be used for both on-premises and cloud applications.

§ **Role-based access control** - Multiple tools in Azure support authorization based on their role, simplifying access control across defined groups of users.

Data Protection Both technological safeguards, such as encrypted communications, and operation processes help keep Customer Data secure. Customers have the flexibility to implement additional encryption and manage their own keys.

Data in transit. Azure uses industry-standard transport protocols such as SSL and TLS between user devices and Microsoft data centers, and within data centers themselves. With virtual networks, customers can use industry standard IPsec protocol to encrypt traffic between their corporate VPN gateway and Azure. Customers can enable encryption for traffic between their own VMs and end users.

§ **Data at rest**. Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to choose the solution that best meets their needs. Options include .NET cryptographic services, Windows Server public key infrastructure (PKI) components, Active Directory Rights Management Services (AD RMS), and BitLocker for data import/export scenarios.

§ **Data segregation**. Azure is a multi-tenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

§ **Data destruction**. When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware.

§ For additional security information refer to the security best practices or Azure Security Insights documents on Microsoft's Azure Trust Center.

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

Globally: CSA-STAR, DFARS, ISO 20000-1:2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 9001, SOC (1,2,3), and WCAG 2.0

US: CJIS, DoD DISA (L2, L4, L5), DoE 10 CFR Part 810, EAR (US Export Administration Regulations), FDA CFR Title 21 Part 11, FedRAMP, FERPA, FIPS 140-2, IRS 1075, ITAR, NIST 800-171, NIST Cybersecurity Framework (CSF), and Section 508 VPATS.

Industry Specific: 23 NYCRR 500, CDSA, FFIEC, CLBA, GxP, HIPAA/HITECH, HITRUST, MARS-E, MPAA, PCI DSS, and SOX.

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Microsoft Azure categorizes logs into the following categories:

Control/management logs which provide information about Azure Resource Manager CREATE, UPDATE, AND DELETE operations.

Data plane logs that provide information about events raised as a part of Azure resource usage. These types of logs are commonly associated with system, security, and application logs in a virtual machine (VM) and the diagnostics logs that are configured through Azure Monitor.

Processed events provide information about analyzed events/alerts that have been processed on the Customer's behalf. Examples of this type are Azure Security Center alerts where Azure Security center has processed and analyzed your subscription and provides concise security alerts.

Microsoft lists the most important log types as the following:

Log category	Log type	Usage	Integration
Activity logs	Control-plane events on Azure Resource Manager resources	Provides insight into the operations that were performed on resources in your subscription.	Rest API, Azure Monitor
Azure diagnostics logs	Frequent data about the operation of Azure Resource Manager resources in subscription	Provides insight into operations that your resource itself performed.	Azure Monitor, Stream
Azure AD reporting	Logs and reports	Reports user sign-in activities and system activity information about users and group management.	Graph API
Virtual machines and cloud services	Windows Event Log service and Linux Syslog	Captures system data and logging data on the virtual machines and transfers that data into a storage account of your choice.	Windows (using Windows Azure Diagnostics [WAD] storage) and Linux in Azure Monitor
Azure Storage Analytics	Storage logging, provides metrics data for a storage account	Provides insight into trace requests, analyzes usage trends, and diagnoses issues with your storage account.	REST API or the client library
Network Security Group (NSG) flow logs	JSON format, shows outbound and inbound flows on a per-rule basis	Displays information about ingress and egress IP traffic through a Network Security Group.	Azure Network Watcher
Application insight	Logs, exceptions, and custom diagnostics	Provides an application performance monitoring (APM) service for web developers on multiple platforms.	REST API, Power BI
Process data / security alerts	Azure Security Center alerts, Azure Log Analytics alerts	Provides security information and alerts.	REST APIs, JSON

https://docs.microsoft.com/en-us/azure/security/azure-log-audit

Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as "audit logs" or "operational logs," because they report control-plane events for the Customer's subscription(s).

Activity logs help you determine the "what, who, and when" for write operations (that is, PUT, POST, or DELETE). Activity logs also help you understand the status of the operation and other relevant properties. Activity logs do not include read (GET) operations.

Azure diagnostics logs are emitted by a resource that provides rich, frequent data about the operation of that resource. The content of these logs varies by resource type. For example, Windows event system logs are a category of diagnostics logs for VMs, and blob, table, and queue logs are categories of diagnostics

logs for storage accounts. Diagnostics logs differ from activity logs, which provide insight into the operations that were performed on resources in your subscription.

The Customer can retrieve events from an activity log by using the Azure portal, Azure CLI, PowerShell cmdlets, and Azure Monitor REST API. Activity logs have 19-day data-retention period.

Azure Active Directory (Azure AD) includes security, activity, and audit reports for a user's directory. The Azure AD audit report helps you identify privileged actions that occurred in the user's Azure AD instance. Privileged actions include elevation changes (for example, role creation or password resets), changing policy configurations (for example, password policies), or changes to the directory configuration (for example, changes to domain federation settings).

Azure Storage Analytics logs and provides metrics data for a storage account. You can use this data to trace requests, analyze usage trends, and diagnose issues with your storage account. Storage Analytics logging is available for the Azure Blob, Azure Queue, and Azure Table storage services. Storage Analytics logs detailed information about successful and failed requests to a storage service.

You can use this information to monitor individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis. Log entries are created only if there are requests made against the service endpoint. For example, if a storage account has activity in its blob endpoint but not in its table or queue endpoints, only logs that pertain to the Blob storage service are created.

Network logging and monitoring in Azure is comprehensive and covers two broad categories:

Network Watcher: Scenario-based network monitoring is provided with the features in Network Watcher. This service includes packet capture, next hop, IP flow verify, security group view, NSG flow logs. Scenario level monitoring provides an end to end view of network resources in contrast to individual network resource monitoring.

Resource monitoring: Resource level monitoring comprises four features, diagnostics logs, metrics, troubleshooting, and resource health. All these features are built at the network resource level.

Network Security Group flow logging - NSG flow logs are a feature of Network Watcher that you can use to view information about ingress and egress IP traffic through an NSG. These flow logs are written in JSON format and show:

Outbound and inbound flows on a per-rule basis.

The NIC that the flow applies to.

5-tuple information about the flow: the source or destination IP, the source or destination port, and the protocol.

Whether the traffic was allowed or denied.

Azure Application Insights is an extensible APM service for web developers on multiple platforms. Use it to monitor live web applications. It automatically detects performance anomalies. It includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.

Azure Security Center threat detection works by automatically collecting security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats. Security alerts are prioritized in Security Center along with recommendations on how to remediate the threat.

Log Analytics is a service in Azure that helps you collect and analyze data that's generated by resources in your cloud and on-premises environments. It gives you real-time insights by using integrated search and custom dashboards to readily analyze millions of records across all your workloads and servers, regardless of their physical location.

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

Azure Active Directory (Azure AD) is a comprehensive identity and access management solution that provides a robust set of capabilities to manage access to on-premises and cloud applications and resources including Microsoft online services like Office 365 and a world of non-Microsoft SaaS applications.

Microsoft Azure offers Federated Authentication and/or Pass-through Authentication for user verification and access authorization.

Once authenticated, Azure Active Directory groups may be used to restrict users' accesses to resources as dictated by the needs of the company. Azure Active Directory may grant or deny access through:

Direct Assignment: Users can be assigned directly to a resource by the owner of that resource.

Group Membership: A group can be assigned to a resource by the resource owner, and by doing so, granting the members of that group access to the resource. Membership of the group can then be managed by the owner of the group. Effectively, the resource owner delegates the permission to assign users to their resource to the owner of the group.

Rule-based: The resource owner can use a rule to express which users should be assigned access to a resource. The outcome of the rule depends on the attributes used in that rule and their values for specific users, and by doing so, the resource owner effectively delegates the right to manage access to their resource to the authoritative source for the attributes that are used in the rule. The resource owner still manages the rule itself and determines which attributes and values provide access to their resource.

External Authority: The access to a resource is derived from an external source; for example, a group that is synchronized from an authoritative source such as an on-premises directory or a SaaS app such as WorkDay. The resource owner assigns the group to provide access to the resource, and the external source manages the members of the group.

External Authority Example:

At the center of the Azure AD access management solution is the security group. Using a security group to manage access to resources is a well-known paradigm, which allows for a flexible and easily understood way to provide access to a resource for the intended group of users. The resource owner (or the

administrator of the directory) can assign a group to provide a certain access right to the resources they own. The members of the group will be provided the access, and the resource owner can delegate the right to manage the members list of a group to someone else, such as a department manager or a helpdesk administrator.

In example:

https://docs.microsoft.com/en-us/azure/active-directory/active-directory-manage-groups

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

CodeLynx Response:

CodeLynx takes security very seriously. As such the CodeLynx Contract Manager will report any security incident regardless of incident level to designated customer's Information Owner and/or Information Systems Security Manager. Both CodeLynx Information Owner and Information Systems Security Managers will work in conjunction with Microsoft's Security team through the Identification, Containment and Eradication phases of a breach and/or confirmed security incident.

Microsoft continuously monitors for information security. Response to incidents start immediately after initial discovery and an Incident Assessment Phase. Notification to customers occurs after an incident is confirmed and constitutes the Customer Notification Phase. During the customer notification phase the Global Administrator for an Azure resource is contacted. If, due to contract specifications, the Global Administrator is a CodeLynx employee and not a client employee, CodeLynx will immediately reach out to the client for notification.

Until the extent of the security incident is confirmed, communications between CodeLynx Inc. and customer will be exclusively through voice communications. Use of email communications is discouraged during the identification phase of the incident.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Operational Security Assurance (OSA) is an important process that Microsoft uses to make its networks more resilient to attack and increase the security of its cloud-based services. OSA helps Microsoft achieve this increased resilience and security by extending the foundation of Microsoft cloud-based services to protect against Internet-based security threats and by incorporating best practices and methodology to continuously update services to improve security and resolve incidents as quickly as possible.

Hyper-scale

With more than 100 datacenters worldwide, Microsoft has datacenters located in every region, connected by one of the largest cloud networks in the world. There are only a few cloud providers who are individually enterprise grade, hybrid, or hyper-scale, but Microsoft's cloud is the only one that offers all three.

The distributed and virtual networks in Azure help ensure that each customer's private network traffic is logically isolated from traffic belonging to other customers. A customer subscription can contain multiple isolated private networks (and include firewall, load-balancing, and network address translation):

Deployment network: Each deployment is isolated from other deployments at the network level. Multiple VMs within a deployment can communicate with each other through private IP addresses.

Virtual network: Each virtual network is isolated from other virtual networks. Multiple deployments (inside the same subscription) can be placed on the same VNET and allowed to communicate through private IP addresses.

By default, Virtual Machines inside the private network do not receive inbound traffic from outside of the deployment. The administrator defines an input endpoint that specifies which ports on which VMs should receive inbound traffic initiated from outside a deployment's isolated network—enabling traffic from the Internet and other deployments or customers inside Azure. Microsoft Azure uses multiple safeguards to protect customer and enterprise data. These security practices and technologies include:

Identity and access management. Azure Active Directory helps ensure that only authorized users can access your environments, data, and applications, and provides multi-factor authentication for highly secure sign-in.

Encryption. Azure uses industry-standard protocols to encrypt data as it travels between devices and Microsoft datacenters, and crosses within datacenters

Secure networks. Azure infrastructure relies on security practices and technologies to connect virtual machines to each other and to on-premises datacenters, while blocking unauthorized traffic. Azure Virtual Networks extend your on-premises network to the cloud via a site-to-site virtual private network (VPN). You can also use ExpressRoute to create a cross-premises connection when needing to use the Internet.

Threat management. Microsoft Antimalware protects Azure services and virtual machines. Microsoft also uses intrusion detection, denial-of-service (DDoS) attack prevention, penetration testing, data analytics, and machine learning to constantly strengthen its defense and reduce risks.

Compliance. We comply with both international and industry-specific compliance standards and participate in rigorous third-party audits, which verify our security controls.

Physical zoning and Virtual Zoning of HOST systems is supported through Microsoft Azures extensive use of Software-Defined Networks which spans across datacenter from edge computing not to the interval fiber backbones.

Physical Access to Facilities. Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.

Physical Access to Components. Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain.

Protection from Disruptions. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

Component Disposal. Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.

With software enablement for restricting access, security is critical to provide customer data and privacy. Microsoft goes beyond ISO and NIST standards to ensure physical and virtually safe environments. As an example, in the Azure infrastructure there is Separation of CPU's Storage, SQL Services that supports greater Zoning and Security requirements.

Software-Defined Networks (In Support of Zoning)

To improve flexibility and accelerate the adoption of advanced technologies into our network, we have broadly adopted a software-defined networking (SDN). SDN provides the ability to dynamically modify our network using automated management tools to move data and resources to an area where it is best served. In an SDN environment, we can extract and separate the application, the control plane, and the transport of the data. This allows us to insert our own APIs to gain visibility of how the data flows and gain better control and allows us to upgrade network performance outside of the hardware refresh cycle. Our large, geographically distributed footprint of datacenters and networks enables us to be located close to our customers to reduce network latency and allow for geo-redundant back-up and failover.

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

In Microsoft's Security Services and Technologies site (https://docs.microsoft.com/en-us/azure/security/azure-security-services-technologies) there are technical reference architectures available for IaaS, PaaS, and SaaS for hundreds of different implementation scenarios. As every client's implementation of the hundreds of services available in the cloud will differ the Security Services and Technologies site is an incredibly useful catalogue for making sure security best practices are followed at all times. The catalogue is updated regularly as new technologies and capabilities are released eliminating security gaps created by using static or stale architectures and plans.

Some sample reference architectures from the extensive catalogue available are provided here below.

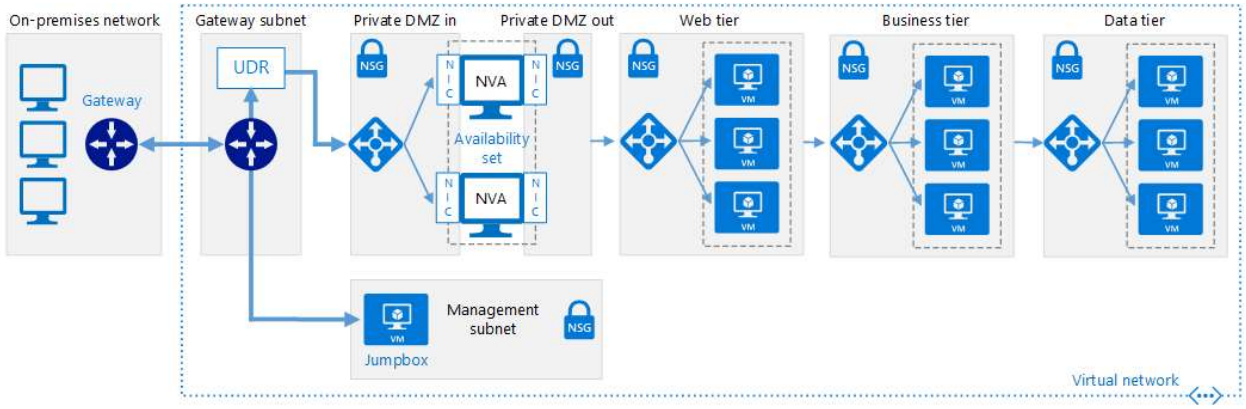


Figure: IaaS DMZ between Azure and your on premise datacenter

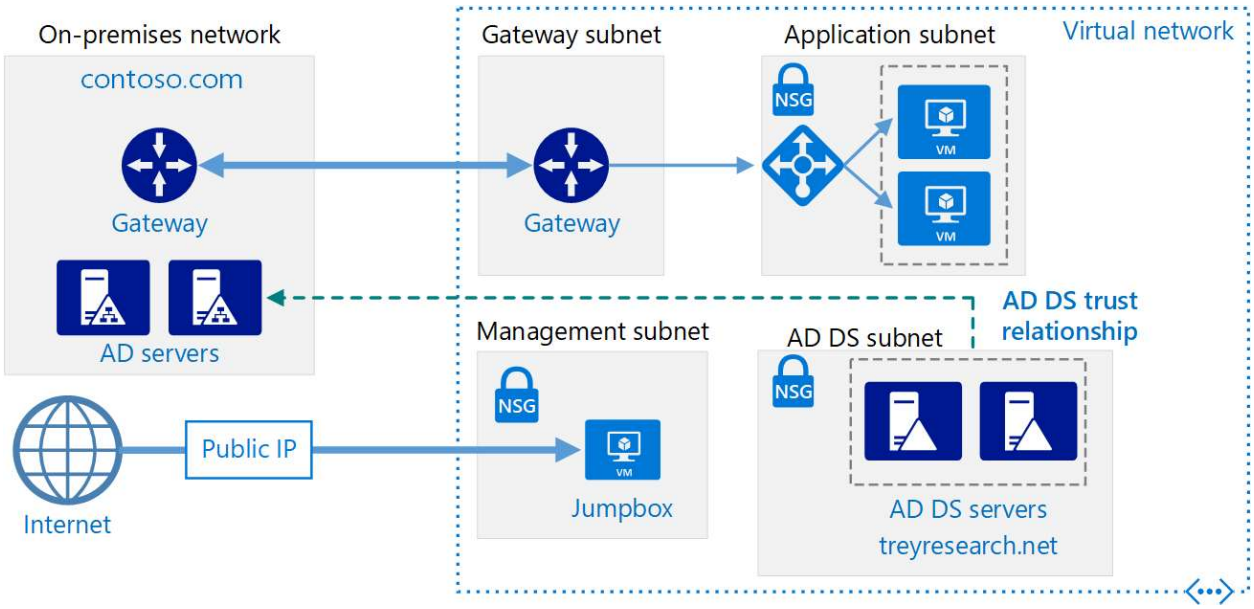


Figure: Creation of an AD DS forest in Azure trusted by on-premise AD forest

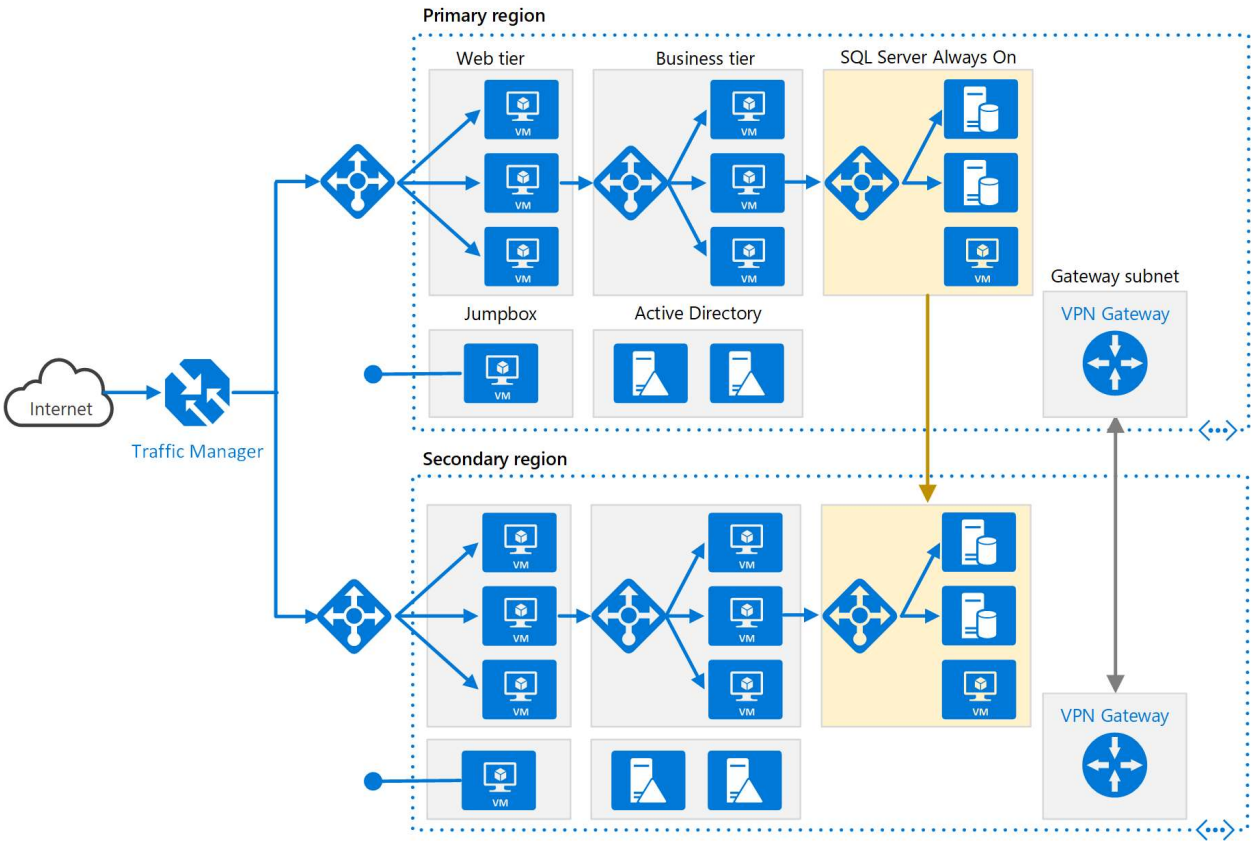


Figure: Multi-region N-tier application for high availability

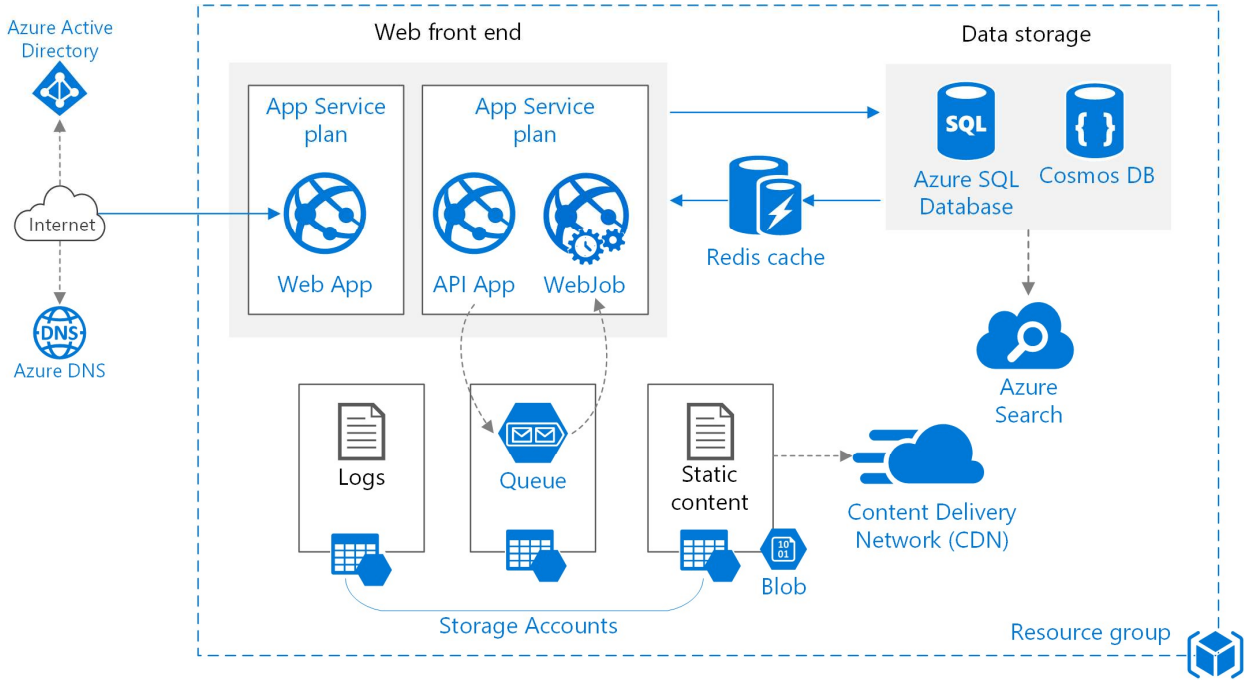


Figure: PaaS architecture for advanced scalability of a web application

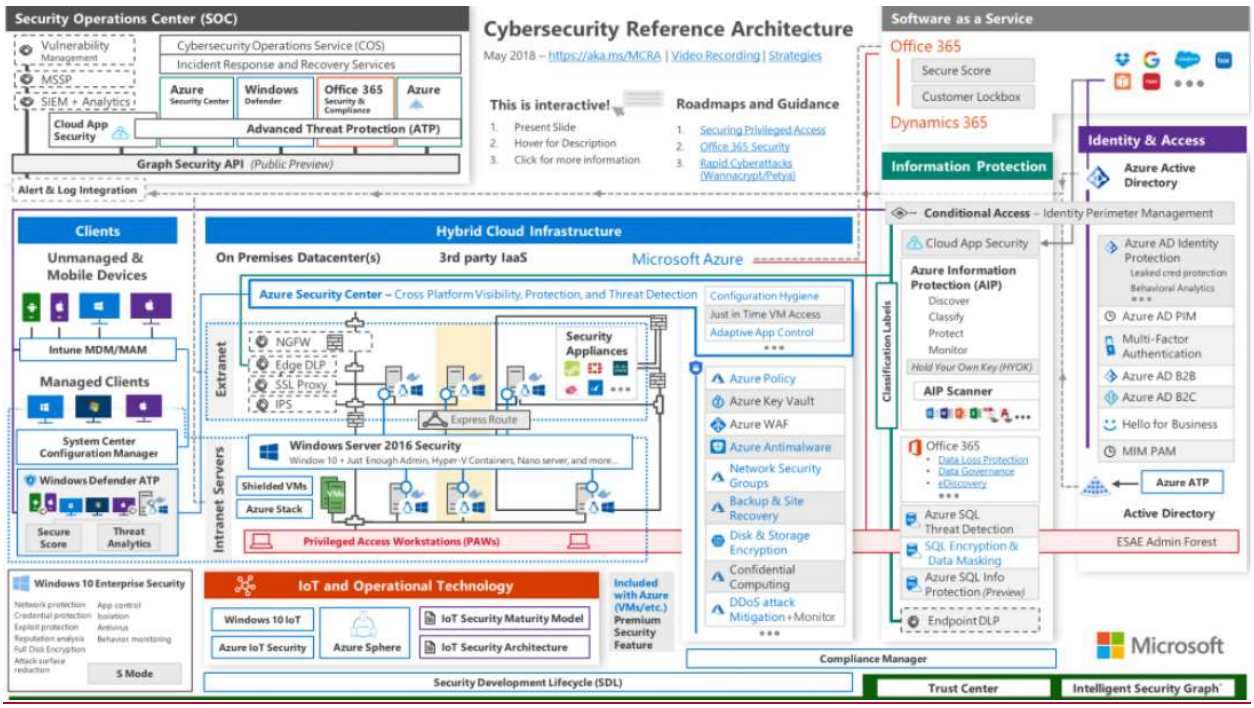


Figure: Representative architecture of a IaaS, PaaS, SaaS integrated security model

As organizations move workloads to the cloud, they must address threats in new ways and shed legacy security practices that often have proven to be ineffective and burdensome. In some cases, extending to the cloud provides an opportunity to implement security controls and contain adversaries in ways that are

more challenging to accomplish in existing on-premises environments. Although containment strategies are not new, the traditional network-centric approach has failed in several ways and needs to be updated.

As such every security architecture should take the following principles in mind.

Containment strategy. High-level strategic approach designed to limit the risk and scope of any given compromise

Segmentation strategy. Component of the containment strategy that separates computing assets into security zones that reflect significantly different asset valuation, trust levels, and/or risk exposure profiles

Security zone. Set of computing assets with a common asset valuation, trust level, and/or risk exposure profile.

The notions of containment and segmentation have been around for a long time in IT security, though the interpretations of how to implement them have varied in practice. This document starts with an assume breach mindset and calls for designing security controls to prevent propagation of breaches among enterprise assets. This requires architects and system designers to look at what a breached system or compromised account means to the environment so as to limit the impact of that breach, to make it detectable, and to enable the organization to respond. This assume breach approach complements the traditional perimeter approach focused on preventing breaches for a combined approach that results in a more resilient strategy.

Each client's implementation will be different and as such an architecture will be created that best fits their scenario and creates the most secure environment that can be offered.

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

CodeLynx Response:

Our Acceptable Use Policy, Facility Clearance, and Insider Threat Program govern the behavior of employees and use of company-issued computing devices used to access client data and maintain our products.

CodeLynx has an Acceptable Use Policy (AUP) in place that applies to all employees with the intention of protecting our employees, partners, clients, and the company from illegal or damaging actions through all internet, intranet, and extranet related systems. Appendix B of the AUP specifically addresses our standards and expectations for how confidential information is treated. Any information provided to us by a client/customer is considered confidential. The AUP stipulates guidelines, defines specific rules, identifies control and compliance measurements, and penalties for non-compliance.

Procedures under this policy include (but are not limited to): storing and locking documents when not in use, encrypting electronic information to safeguard local databases on their personal devices, signing non-compete and/or non-disclosure agreements. Access to confidential information is approved by the project manager and granted/controlled through restricting network/share drive access to those with a "need to know." If an employee believes they may need additional access to confidential information to complete job duties and/or assigned tasks, they are required to request authorization from management. Adherence to this policy is verified through a variety of methods which include (but are not limited to): periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

In addition to a robust AUP, CodeLynx has a US Government Facility Clearance, which is overseen by the Department of Defense, Defense Security Service (DoD-DSS). As a cleared defense contractor since 2009, CodeLynx is experienced with the security requirements of government clients. We possess a "Secret (non-holding)" facility clearance and have been consistently assessed as "Commendable" by the DoD-DSS. Our security staff are familiar with the processes for initiating, monitoring, and following through on the wide variety of personal security requirements which include: initial and periodic investigations, background checks, adjudication, fingerprinting, visit requests, testing for prohibited substances, acquisition of government or client credentials, training, and any other administrative requirements that are necessary or prudent.

As part of our Insider Threat Program, CodeLynx encourages the reporting of suspicious behavior, activity, communications, and provides training on how to recognize and contain spillage of sensitive information. The Insider Threat Program Plan applies to all staff offices, regions, and personnel with access to any company, government, or contractor resources to include personnel, facilities, information, equipment, networks, or systems. The program gathers, integrates, and reports relevant and credible information that may be indicative of a potential or actual insider threat to deter all employees from becoming insider threats; detect any person with authorized access to any client or company resources to include personnel, facilities, information, equipment, networks, or systems, who pose a risk to sensitive information; and mitigate the risk of an insider threat as defined above.

CodeLynx employs the security concept of "Least Privileges" to ensure that applications and personnel only access the information and resources that are necessary for its legitimate purpose. This is enforced through limitation of access to project folders on networks/share drive/portals to members of that project team.

All client information provided to CodeLynx will be logged by the Security Team upon receipt. Due to the inherent nature of "client information," we believe we do not possess the authority to determine the outcome of data or material that does not belong to the company. Client information will not be shared, replicated, deleted or destroyed without approval.

Sensitive information in paper or physical form (i.e. electronic storage media) will be stored in our GSA approved security container (class 6 filing cabinet). CodeLynx security personnel will log the information in and out of the safe, which will remain locked unless being accessed. The information will be viewed/used in an area and manner such that it is not susceptible to unauthorized disclosure (intentional or otherwise).

While CodeLynx employs multiple redundant methods to prevent the loss of sensitive information, the company also has a Security Incident Response Plan in place. This combination of policy and procedure contains specific checklists for conducting the response process. Our methodology follows the seven steps outlined in the NIST incident response process: prepare, detect, analyze, contain, eradicate, recover, and record. We emphasize that every employee is trained to recognize and empowered to report a trigger event that would lead us to put our Security Incident Response Plan into action.

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Microsoft Personnel. Microsoft personnel will not process Customer Data without authorization from Customer. Microsoft personnel are obligated to maintain the security and secrecy of any Customer Data as provided in the DPT and this obligation continues even after their engagements end.

Subcontractor Transfer. Microsoft may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Each Online Service has a website that lists subcontractors that are authorized to access Customer Data as well as the limited or ancillary services they provide. At least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent Customer invoices.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

Microsoft encrypts customer data at transit and at rest and provides a complaint platform to NIST standards. Industry and government regulations such as HIPAA and FedRAMP, and international standards such as ISO 27001, lay out specific safeguards through processes and policies. It is a shared responsibility between Microsoft Azure and its customers to implement sufficient mechanisms to meet those obligations. Specifically, Microsoft provides a compliant platform for services, applications, and data, while Azure customers must design and configure their cloud environment to ensure the confidentiality and integrity of their information assets.

There are multiple tools within Microsoft Azure to safeguard data according to your company's security and compliance needs. One of the keys to data protection in the cloud is accounting for the possible states in which your data may occur, and what controls are available for that state. Specifically:

At Rest. This includes all information storage objects, containers, and types that exist statically on physical media, be it magnetic or optical disk.

In Transit. When data is being transferred between components, locations or programs, such as over the network, across a service bus (from on-premises to cloud and vice-versa, including hybrid connections such as ExpressRoute), or during an input/output process, it is thought of as being in-motion. Being in-transit does not necessarily mean a communications process with a component outside of your cloud service; it moves internally, also, such as between two virtual networks.

I**n Use or In Process**. Dynamic data usage could be a table kept in virtual memory, transactions in a message queue, or even encryption keys in the CPU cache. Information being acted upon in some way by the host or guest during a process, such as real-time database queries running in active memory (as opposed to a

page file sent out to disk), could be in different security states depending on whether it is encrypted or decrypted, and the security context of the operator.

Further, there are two (2) fundamental types of data at rest:

Data in production. There is data in some form of storage, e.g. Azure SQL Database, and compute processes that need to access that storage during production operations. In this case, encryption at rest is aimed at protecting the data in that storage (whereas the compute aspect deals with data in use).

Data not in production. There is data in some form of storage, e.g. a Virtual Hard Disk (VHD), but that VHD is not in production use. For example, it may be part of an upgrade operation, but the VHD has not yet been loaded or mounted. Data encryption at rest is applicable here, but the compute aspect is not relevant for this scenario.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

CodeLynx Response:

Notification of Breach

1. Upon notification of a breach the Privacy Officer will work with the department(s) involved, CodeLynx's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law within the state whose data was breached.
2. Notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened
            2. Types of Card Holder information and/or PII/PHI involved
            3. Steps individuals should take
            4. Steps covered entity is taking
            5. Contact Information
            6. Date of Breach
        ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
    b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, CodeLynx's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals and applicable state laws require it, or contact information is insufficient, CodeLynx will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.

5. Using multiple methods of notification in certain cases may be the most effective approach.

Mitigating the Breach

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
    a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
        i. Stopping the unauthorized practice
        ii. Recovering the records, if possible
        iii. Shutting down the system that was breached
        iv. Mitigating the breach, if possible
        v. Correcting weaknesses in security practices
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity
2. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
3. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
4. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
5. The resulting plan will also include audit recommendations, if appropriate.

8.7 Migration and Redeployment Plan

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

Microsoft is governed by strict standards and follows specific processes for removing cloud customer data from systems under our control, overwriting storage resources before reuse, and purging or destroying decommissioned hardware.

Data retention

In our Online Services Terms, Microsoft contractually commits to specific processes when a customer leaves a cloud service, or the subscription expires. This includes deleting customer data from systems under our control.

If you terminate a cloud subscription or it expires (except for free trials), Microsoft will store your customer data in a limited-function account for 90 days (the "retention period") to give you time to extract the data

or renew your subscription. During this period, Microsoft provides multiple notices, so you will be amply forewarned of the upcoming deletion of data.

After this 90-day retention period, Microsoft will disable the account and delete the customer data, including any cached or backup copies. For in-scope services, that deletion will occur within 90 days after the end of the retention period. (In-scope services are defined in the Data Processing Terms section of our Online Services Terms.)

When customer data is hosted in the multitenant environments of Microsoft business cloud services, we take careful measures to logically separate customer data. This helps prevent one customer's data from leaking into that of another customer, which also helps to block any customer from accessing another customer's deleted data.

Data deletion on physical storage devices

If a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. The data on the drive is completely overwritten to ensure that the data cannot be recovered by any means.

When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

At all times during the term of Customer's subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data. The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data as described in this section.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

The customer's use of any Import/Export Service is conditioned upon its compliance with all instructions provided by Microsoft regarding the preparation, treatment and shipment of physical media containing its data ("storage media"). The customer is solely responsible for ensuring the storage media and data are provided in compliance with all laws and regulations. Microsoft has no duty with respect to the storage media and no liability for lost, damaged or destroyed storage media. All storage media shipped to Microsoft must be shipped DAP Microsoft DCS Data Center (INCOTERMS 2010). Storage media shipped to Customer will be shipped DAP Customer Dock (INCOTERMS 2010).

Migration and redeployment is not part of solutions CodeLynx is offering in this response.

As for return of data, Microsoft's approach is to provide self-service access to its customer's administrators to extract data upon termination. Regarding Office 365 Services, Microsoft Azure Core Services, Microsoft Dynamics CRM Online Services, and Microsoft Intune Online Services (as each is defined in the Microsoft Online Service Terms, or "OST"), Microsoft provides Customer administrators access to their Customer Data in the Online Services at all times during the term the subscription, and for at least 90 days thereafter (but

for no more than 180 days). Where the modality of the Online Service is applicable and as described in the applicable service documentation and service descriptions at the time, Customer Data in the Online Services will be downloadable by the State in a common industry or published Microsoft format (e.g. MS Outlook PST files, MS Office document files in the then-current format,, MS SQL Database files, CSV format files) , during the term of each subscription and for a 90-day "limited functionality" period following expiration (as set forth in the Online Services Terms). For some Online Services service components (also variously described as workloads, services, or modules in Microsoft documentation) download is not possible (such as when the module provides for functionality to synchronize from primary copies of Customer Data held and maintained by the customer), or Customer is intended by the component design to prepare and develop or configure their own download modality (such as when Microsoft provides a platform for Customers own applications to be run as a cloud service).

8.8 Service or Data Recovery

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.

b. Suffers an unrecoverable loss of data.

c. Offeror experiences a system failure.

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

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

CodeLynx Response:

In the event of an outage, transparency is critical. In all cases involving service outage, CodeLynx will inform the affected Purchasing Entities as soon as possible. Throughout the recovery process, CodeLynx will update Purchasing Entities with status, possible options, and expected recovery time. See below for information about specific cases.

Microsoft Azure's Business Continuity Plans (BCP) have been documented and published for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum.

Microsoft's BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.

Extended Downtime: In the case of extended downtime, CodeLynx works with Purchasing Entities to make decisions about whether to activate disaster recovery and continuity planning or to continue to wait for restoration. If disaster recovery and continuity plans are activated, storage and data backup choices are important to consider.

Purchasing Entities using an IaaS infrastructure can leverage Microsoft Azure Backup to back up their Microsoft SQL Server, Hyper-V VMs, SharePoint Server, Microsoft Exchange, and Windows clients. Additional detailed information about Microsoft Azure Backup can be found at the following website: https://docs.microsoft.com/en-us/azure/backup/

Purchasing Entities using a PaaS infrastructure should implement database backup policies that create database backups on a regular interval and then ship the backups to a Microsoft Storage account that resides in a separate geographic location from the application. Application code can also be backed up to the storage account or it can be managed through the Purchasing Entities' own code repository.

If availability is a concern, Purchasing Entities can quickly use their backups to create a new instance of their application or system running either in the same region or a different one, in case of a regional outage.

Unrecoverable loss of data: CodeLynx understands an unrecoverable loss of data as an unavoidable situation where a corruption has occurred, and the data is therefore lost. As these events are not preventable, we believe that the best solution is for the Purchasing Entities to create solid, tested backup plans. If unrecoverable data loss is a concern, Purchasing Entities should implement backup and disaster recovery resources and procedures to ensure that frequent data backups are available, limiting the impact of such a loss.

Offeror system failure: In the event of a system failure, we will execute one of Microsoft's disaster recovery options. The most effective option is changing the region or data center to resume operations. Once operations have resumed, the primary computing environment can be assessed and recovered. Once tested, Purchasing Entities can choose to migrate their users back to the primary computing environment.

Recovering and restoring data within four business hours: Creating plans and automated processes that back up resources on a reasonable, organization-specified interval can protect Purchasing Entities' resources that have been identified as needing to be restored within a four-hour period. For IaaS customers, Microsoft Azure offers Disaster Recovery as a Service in their Site Recovery product, which a Purchasing Entity can use to automate the recovery of services affected by an outage at the primary data center. Site Recovery can protect Hyper-V, VMware and physical servers using an Azure secondary data center as a recovery site.

Recovery Point Objective (RPO) and Recovery Time Objective (RTO): CodeLynx understands that needs vary, not only across companies, but also across products. We will work closely with Purchasing Entities to determine the RPO and RTO that make the most sense for the Entities' needs. CodeLynx will provide detailed information on how to achieve RPO and RTO, listing specific resources that may be required so that the Purchasing Entities clearly understand both how to implement proper disaster recovery methods and its financial impact.

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

a. Method of data backups

b. Method of server image backups

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

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

CodeLynx Response:

Backup and restore services for Microsoft Azure and Microsoft Azure Government offerings are detailed below.

Azure Backup is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure. See the table below for information about which component to use to protect specific data, applications, or workloads.

Component	Benefits	Limits	What is protected?	Where are backups stored?
Azure Backup (MARS) agent	Back up files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure) No separate backup server required.	Backup 3x per day Not application aware; file, folder, and volume-level restore only, No support for Linux.	Files, Folders, System State	Recovery Services vault
System Center DPM	Application-aware snapshots (VSS) Full flexibility for when to take backups Recovery granularity (all) Can use Recovery Services vault Linux support on Hyper-V and VMware VMs Back up and restore VMware VMs using DPM 2012 R2	Cannot back up Oracle workload.	Files, Folders, Volumes, VMs, Applications, Workloads System State	Recovery Services vault, Locally attached disk, Tape (on-premises only)
Azure Backup Server	Application-aware snapshots (VSS) Full flexibility for when to take backups Recovery granularity (all) Can use Recovery Services vault Linux support on Hyper-V and VMware VMs Back up and restore	Cannot back up Oracle workload. Always requires live Azure subscription No support for tape backup	Files, Folders, Volumes, VMs, Applications, Workloads, System State	Recovery Services vault, Locally attached disk

	VMware VMs Does not require a System Center license			
Azure IaaS VM Backup	Application-aware snapshots (VSS) Native backups for Windows/Linux No specific agent installation required Fabric-level backup with no backup infrastructure needed	Back up VMs once-a-day Restore VMs only at disk level Cannot back up on-premises	VMs, All disks (using PowerShell)	Recovery Services vault

Table: Azure Backup Components

Microsoft Azure features the following data center regions within the United States:

East US

East US 2

Central US

North Central US

South Central US

West Central US

West US

West US 2

Microsoft Azure Government features the following data center regions within the United States:

US DoD East

US DoD Central

US Gov Arizona

US Gov Iowa

US Gov Texas

US Gov Virginia

8.9 Data Protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

The types of encryption technologies and the responsibility of implementation will vary based on our client's service model; IaaS, PaaS, SaaS. Specific technologies and best practices may be found at source: https://docs.microsoft.com/en-us/azure/security/security-azure-encryption-overview

Microsoft published Protecting Data in Microsoft Azure (http://download.microsoft.com/download/0/d/d/0dd8fb12-6343-4a50-80b2-545f2951d7ae/microsoftazuredataprotection_aug2014.pdf) to provide a "how-to" and outline the data benefits that are provided through multiple layers of security and governance technologies.

Data Security in Azure AD

Sensitive identity information stored in Azure AD is protected through the following means:

Data in transit: All customer facing Web services are secured with SSL/TLS. All LDAP and partition / replication traffic to and within the directory store (within and between datacenters) is signed.

Data at rest: When at rest, secrets stored in the directory (symmetric keys, private asymmetric keys, passwords) are encrypted using the Distributed Key Manager (DKM).

By default, Windows Azure AD disallows all operations issued by identities in other tenants. A tenant administrator may explicitly grant directory access to identities from other tenants, if desired.

Platform Encryption

Among Microsoft Azure's data protection capabilities are built-in services, components and configurations that apply encryption to internal data and traffic. These serve to enable enhanced security for customer information, and also help enforce data governance and compliance with industry regulations (and are mandated as such).

Many of these mechanisms are enabled by default in the platform while others need to be configured by a customer administrator (such as IPsec VPN). Some can be optionally invoked at VM boot-time through service configuration files or called by application components directly.

Azure implements encryption using both symmetric and asymmetric keys for encrypting and protecting confidentiality of data:

Software-based AES-256 for symmetric encryption/decryption

2048-bit or better for asymmetric keys

SHA-256 or better for secure hashing

Encryption in Transit

Microsoft Azure uses virtual networking to isolate tenants' traffic from one another, employing measures such as host- and guest-level firewalls, IP packet filtering, port blocking, and HTTPS endpoints. However, most of Azure's internal communications, including infrastructure-to-infrastructure and infrastructure-to-customer (on-premises), are also encrypted.

For communications within an Azure datacenter, Microsoft manages networks to assure that no VM can impersonate or eavesdrop on the IP address of another. TLS/SSL is used when accessing Azure Storage or SQL Databases, or when connecting to Cloud Services. In this case, the customer administrator is responsible for obtaining a TLS/SSL certificate and deploying it to their tenant infrastructure

VM to VM - Data traffic moving between Virtual Machines in the same deployment or between tenants in a single deployment via Microsoft Azure Virtual Network can be protected through encrypted communication protocols such as HTTPS, SSL/TLS, or others.

Data leaving a customer's Cloud Service should be considered Internet-facing, and so appropriate safeguards such as HTTPS or VPN are recommended.

Customer to Cloud - Moving data into and out of your cloud environment is protected through the options available in Azure. This includes management operations, data transfers, and key provisioning. Customers can optionally configure TLS/SSL for defense-in-depth on their Virtual Networks; TLS/SSL is mandatory when accessing the Azure Portal or System Management API (SMAPI).

For small amounts of data, connections directly to your Azure Virtual Network can be made over encrypted connections, such as by an IPsec VPN into your tenant environment; larger data sets can be moved over an isolated high-speed channel such as the new ExpressRoute feature. If ExpressRoute is being used, you can encrypt the data at the application-level using TLS/SSL or other protocols for added protection.

In addition, when interacting with Azure Storage through the Azure Portal, all transactions occur via HTTPS. Storage REST API over HTTPS can also be used to interact with Azure Storage and Azure SQL Database. When populating data into Azure SQL Database, you can encrypt information before it is copied over. Note that data only remains encrypted until it is used and placed in memory on the Azure SQL Database compute node, at which point it exists in an unencrypted state.

Data at Rest

Data at rest will vary by service implementation type. For example, Customers may secure data at rest in an IaaS scenario by encrypting the virtual hard disk (VHD) files. Microsoft and third-party mechanisms are used. Workloads (such as SQL Server) also support Transparent Data Encryption (TDE). Technologies that assist with this are:

Key Vault

SQL Server Transparent Data Encryption

Azure Disk Encryption

Third-party virtual machine volume encryption

Volume Level Encryption

In general, cryptography consists of encryption/decryption, key management (e.g. key lifecycle), and key security. Windows operating systems provide encryption routines (.NET CAPI, CNG) that enable customers to encrypt data before storing it in Azure, and these same mechanisms can also be used within Azure VMs.

The ultimate choice of where you should do your encryption / decryption (in the cloud, on-premises, in-application, on the client, etc.) will depend on the level of control you need to maintain, the cost you are willing to incur (e.g., performance, administration), the confidentiality that must be kept, and the potential for incurring risk. Table 6 below provides an overview of common options.

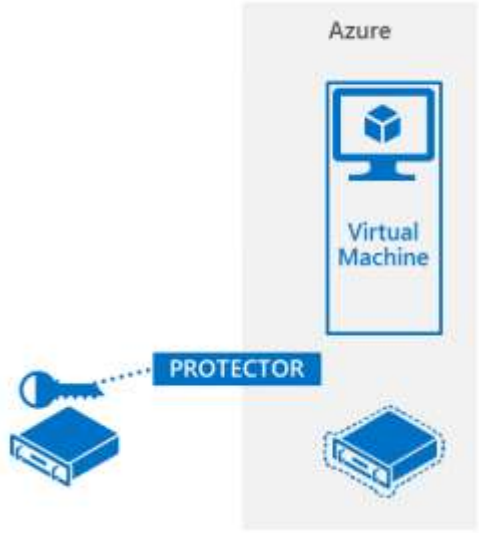
	LAYER	ENCRYPTION SUPPORT	KEY MANAGEMENT	DETAILS
TRANSPARENT DATA	**Application**	.NET Cryptography API	Managed by customer	.NET Cryptography documentation
		Encrypt data using RMS SDK	Managed by customer via on-premises ADRMS service or Azure RMS	RMS SDK documentation
	Platform	SQL TDE/CLE on SQL Server on Azure IAAS VMs	Managed by customers	SQL TDE/CLE documentation
		StorSimple provides primary, backup, archival	Managed by customers	More Information
	System	EFS, BitLocker support for data and boot volumes	Managed by customers	BitLocker command-line tool
	Others	Import/Export of data onto drives can be protected by BitLocker	Managed by customers	Import/export step by step blog

BitLocker Drive Encryption

Azure Virtual Machines are typically associated with storage disks (VHDs) which are in turn stored in Azure Storage. In Azure Storage, data is broken into small chunks and each small chunk is striped across multiple physical disks, providing safeguards against loss of that disk. Additional protection such as drive encryption can be used to mitigate threats such as a compromise of a SAK (used by a VHD). With encrypted disks, even when an unauthorized user obtains the key and in turn uses the key to fetch the VHD from Azure Storage, the VHD is encrypted and thus makes the data unreadable.

Windows offers Full Disk Transparent Encryption through BitLocker for Data Volumes and Boot Volumes, which is transparent to the application. The same BitLocker Drive Encryption (BDE) can be implemented for Azure VMs and VHDs using command line tools such as 'manage-bde'. BitLocker enables volume encryption through several different protectors, such as passwords and certificates. As shown in Figure 11. Azure PowerShell will allow you to remotely execute encryption commands using 'manage-bde', or encryption can be controlled by startup scripts. An auto-unlock feature in BitLocker allows you to unlock the volume automatically without an interactive session.

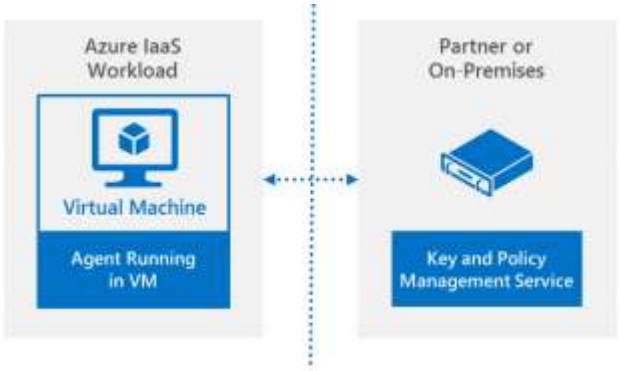
Keys can be protected using on-premises key management services including Hardware Security Modules (HSMs). In Azure VMs, boot volumes can also be encrypted using BitLocker.



Drive Encryption – Partners

Partners such as Trend Micro and others offer volume-level encryption, and manage policies surrounding encryption. These partner solutions also integrate with third-party HSMs and offer solutions for both Windows and Linux VMs. Encryption is transparent to the OS and the applications; thus applications do not need to be changed.

While the implementation of the solutions can vary, an agent typically 'sits' in the OS stack between the disk driver and the file system driver, encrypting the data. Encryption persists even after the instance is stopped.



Key Management and Security

Encryption and authentication do not improve security unless the keys themselves are well protected. It is generally considered a critical IT security task to manage key lifecycles, as proper key management is important to maintaining high security, high reliability, and low overhead.

Encryption key management is left to the implementation of the end-customer. Customers can develop a secure architecture that works for their solutions and have full control over data encryption.

Subscription and Service Certificates

The Azure platform builds on the straightforward key management methods incorporated into the Windows security model, providing the ability to use certificates to secure data (both Virtual Machines and Cloud Services can use any cryptographic facilities in Windows, including those in .NET, CAPI, and CNG).

The main type of certificate that plays a role in securing customer applications or services are called Service Certificates. These are traditional SSL certificates (uploaded by the customer) used to secure endpoint communications. Service certificates can also be used for other purposes, such as Public-Key Cryptography Standards (PKCS)-encrypting data, or to encrypt secret configuration information such as Storage Access Keys.

Azure provides each subscription with an associated logical certificate store that enables automatic deployment of service-specific certificates, and to which customers can upload their own. The certificate store is independent of any hosted service, so it can store certificates regardless of whether they are currently being used by any of those services. These certificates and other credentials uploaded to Azure are stored in encrypted form.

Azure also provides an administrative path to upload certificates and private keys, but not to retrieve private keys. Customer secrets, including certificates, private keys, RDP passwords and SAKs are communicated through the SMAPI via Representational State Transfer (REST)-based protocols or the Azure Portal using SSL.

Certificates and private keys are stored in an encrypted form in Azure on the Fabric Controller. Customer certificates can be directed to customer VMs where they are automatically installed in non-exportable form. Certificates can be managed separately from services and may even be managed by different individuals. For example, a developer may upload a service package that refers to certificates that an IT manager has previously uploaded to the Azure secret store. The IT manager can manage and renew those certificates without stopping the service or uploading a new service package.

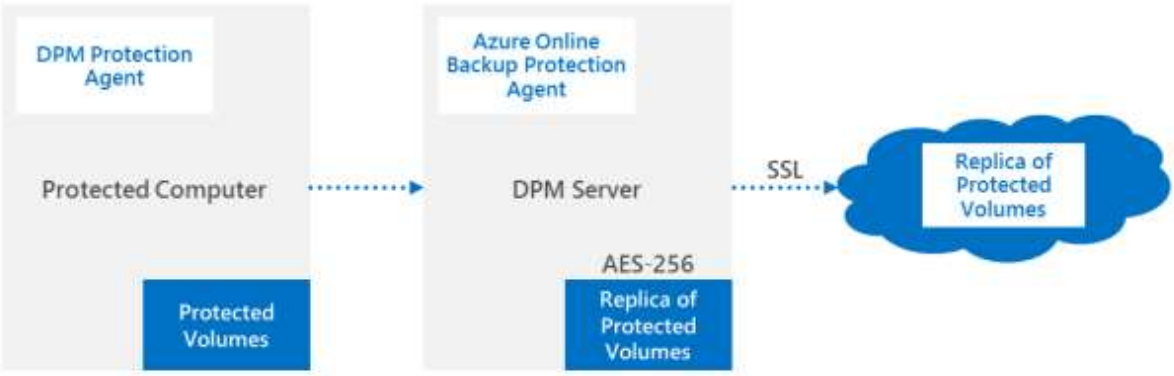
Encryption for SQL Server in Azure Virtual Machines

SQL Server Transparent Data Encryption (TDE) is a proven mechanism for providing storage encryption for on-premises SQL Server 2008 and above installations. TDE is set up through SQL Server configuration and requires no application changes, providing protection from physical storage device theft as well as logical breaches where access to the file system is gained and database files are exposed. More details on SQL Server TDE can be read here.

SQL Server Column-Level Encryption (CLE) offers a more granular level of encryption where data is not decrypted until it is used (conversely, TDE encrypts the entire database in storage, and then decrypts each page in the database fully when it is accessed). Therefore, even if a page is loaded in memory, sensitive data is not in the clear until SQL Server processes it. CLE does require the calling application to be modified to encrypt and decrypt data written to tables. Also, there are performance implications associated with it that customers should consider, as encryption does affect query optimization on the encrypted columns. For this reason, CLE is usually used when the data to be encrypted is small or there are other custom design requirements.

Azure Backup

Azure Backup works with the System Center 2012 Data Protection Manager (DPM) disk-based protection feature. When you enable online protection, the disk-based replicas are backed up to an online location. Backups of your on-premises datacenter servers (or cloud services) are encrypted before transmission and stored encrypted in Azure using AES-256. Backups by the Windows file system and through DPM are similarly encrypted automatically. You can optionally use Windows Server File Classification Infrastructure (FCI) for an additional level of protection by identifying sensitive files for a rights management process, such as Azure RMS.



8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

CodeLynx Response:

CodeLynx is willing to sign relevant and applicable Business Associate Agreements or any other agreement that may be necessary to protect data with a Purchasing Entity.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Customer Data will be used only to provide a Purchasing Entity the Online Services including purposes compatible with providing those services. CodeLynx and Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, the Purchasing Entity retains all right, title and interest in and to Customer Data. Neither CodeLynx nor Microsoft acquires any rights in Customer Data, other than the rights Customer grants to Offeror and Microsoft, to provide the Online Services to Customer. This paragraph does not affect Microsoft's rights in software or Online Services Microsoft licenses to Purchasing Entity.

8.10 Service Level Agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

CodeLynx Response:

CodeLynx's Service Level Agreements (SLA) are inherited from Microsoft Azure and Microsoft Azure Government. The SLAs provided are nonnegotiable. Per Microsoft, if the SLA is not met, a service credit will be offered based on the month of non-compliance. However, additional resources can be provisioned to effectively increase SLA coverage. Purchasing Entities must note that provisioning additional resources to act as backup sites incurs additional costs, which will be clearly defined upon request.

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

CodeLynx Response:

CodeLynx's Service Level Agreements (SLA) are inherited from Microsoft Azure and Microsoft Azure Government. The SLAs provided are nonnegotiable. Per Microsoft, if the SLA is not met, a service credit will be offered based on the month of non-compliance. However, additional resources can be provisioned to effectively increase SLA coverage. Purchasing Entities must note that provisioning additional resources to act as backup sites incurs additional costs, which will be clearly defined upon request.

Service Level Agreements may be subject to change over time. All applicable and current Service Level Agreements can be found on the Microsoft Azure website (https://azure.microsoft.com/en-us/support/legal/sla/). Microsoft's SLA for App Services is presented below as a sample.

SLA for App Service

Last updated: July 2016

We guarantee that Apps running in a customer subscription will be available 99.95% of the time. No SLA is provided for Apps under either the Free or Shared tiers.

Introduction

This Service Level Agreement for Microsoft Online Services (this "SLA") is a part of your Microsoft volume licensing agreement (the "Agreement"). Capitalized terms used but not defined in this SLA will have the meaning assigned to them in the Agreement. This SLA applies to the Microsoft Online Services listed herein (a "Service" or the "Services") but does not apply to separately branded services made available with or connected to the Services or to any on-premises software that is part of any Service.

If we do not achieve and maintain the Service Levels for each Service as described in this SLA, then you may be eligible for a credit towards a portion of your monthly service fees. We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, the version of this SLA that is current at the time of renewal will apply throughout your renewal term. We will provide at least 90 days' notice for adverse material changes to this SLA.

General Terms

Definitions

"**Applicable Monthly Period**" means, for a calendar month in which a Service Credit is owed, the number of days that you are a subscriber for a Service.

"**Applicable Monthly Service Fees**" means the total fees actually paid by you for a Service that are applied to the month in which a Service Credit is owed.

"**Downtime**" is defined for each Service in the Services Specific Terms below.

"**Error Code**" means an indication that an operation has failed, such as an HTTP status code in the 5xx range.

"**External Connectivity**" is bi-directional network traffic over supported protocols such as HTTP and HTTPS that can be sent and received from a public IP address.

"**Incident**" means (i) any single event, or (ii) any set of events, that result in Downtime.

"**Management Portal**" means the web interface, provided by Microsoft, through which customers may manage the Service.

"**Service Credit**" is the percentage of the Applicable Monthly Service Fees credited to you following Microsoft's claim approval.

"**Service Level**" means the performance metric(s) set forth in this SLA that Microsoft agrees to meet in the delivery of the Services.

"**Service Resource**" means an individual resource available for use within a Service.

"**Success Code**" means an indication that an operation has succeeded, such as an HTTP status code in the 2xx range.

"**Support Window**" refers to the period during which a Service feature or compatibility with a separate product or service is supported.

Terms

Claims
In order for Microsoft to consider a claim, you must submit the claim to customer support at Microsoft Corporation including all information necessary for Microsoft to validate the claim, including but not limited to: (i) a detailed description of the Incident; (ii) information regarding the time and duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence.

For a claim related to Microsoft Azure, we must receive the claim within two months of the end of the billing month in which the Incident that is the subject of the claim occurred. For claims related to all other Services, we must receive the claim by the end of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 15th, we must receive the claim and all required information by March 31st.

We will evaluate all information reasonably available to us and make a good faith determination of whether a Service Credit is owed. We will use commercially reasonable efforts to process claims during the subsequent month and within forty-five (45) days of receipt. You must be in compliance with the Agreement

in order to be eligible for a Service Credit. If we determine that a Service Credit is owed to you, we will apply the Service Credit to your Applicable Monthly Service Fees.

If you purchased more than one Service (not as a suite), then you may submit claims pursuant to the process described above as if each Service were covered by an individual SLA. For example, if you purchased both Exchange Online and SharePoint Online (not as part of a suite), and during the term of the subscription an Incident caused Downtime for both Services, then you could be eligible for two separate Service Credits (one for each Service), by submitting two claims under this SLA. In the event that more than one Service Level for a particular Service is not met because of the same Incident, you must choose only one Service Level under which to make a claim based on the Incident. Unless as otherwise provided in a specific SLA, only one Service Credit is permitted per Service for an Applicable Monthly Period.

Service Credits

Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA. You may not unilaterally offset your Applicable Monthly Service Fees for any performance or availability issues.

Service Credits apply only to fees paid for the Service, Service Resource, or Service tier for which a Service Level has not been met. In cases where Service Levels apply to individual Service Resources or to separate Service tiers, Service Credits apply only to fees paid for the affected Service Resource or Service tier, as applicable. The Service Credits awarded in any billing month for a Service or Service Resource will not, under any circumstance, exceed your monthly service fees for that Service or Service Resource, as applicable, in the billing month.

If you purchased Services as part of a suite or other single offer, the Applicable Monthly Service Fees and Service Credit for each Service will be pro-rated.

If you purchased a Service from a reseller, you will receive a service credit directly from your reseller and the reseller will receive a Service Credit directly from us. The Service Credit will be based on the estimated retail price for the applicable Service, as determined by us in our reasonable discretion.

Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center);

That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;

Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised;

During or with respect to preview, pre-release, beta or trial versions of a Service, feature or software (as determined by us) or to purchases made using Microsoft subscription credits;

That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;

That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;

That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);

That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behavior;

Due to your use of Service features that are outside of associated Support Windows; or

For licenses reserved, but not paid for, at the time of the Incident.

Services purchased through Open, Open Value, and Open Value Subscription volume licensing agreements, and Services in an Office 365 Small Business Premium suite purchased in the form of a product key are not eligible for Service Credits based on service fees. For these Services, any Service Credit that you may be eligible for will be credited in the form of service time (i.e., days) as opposed to service fees, and any references to "Applicable Monthly Service Fees" is deleted and replaced by "Applicable Monthly Period."

SLA details

Additional Definitions

"**Deployment Minutes**" is the total number of minutes that a given App has been set to running in Microsoft Azure during a billing month. Deployment Minutes is measured from when the App was created, or Customer initiated an action that would result in running the App to the time Customer initiated an action that would result in stopping or deleting the App.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Apps deployed by Customer in a given Microsoft Azure subscription during a billing month.

"**App**" is a Web App, Mobile App, API App or Logic App deployed by Customer within the App Service, excluding apps in the Free and Shared tiers.

Downtime: The total accumulated Deployment Minutes, across all Apps deployed by Customer in a given Microsoft Azure subscription, during which the App is unavailable. A minute is considered unavailable for a given App when there is no connectivity between the App and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

Monthly Uptime % = (Maximum Available Minutes-Downtime)/(Maximum Available Minutes) x 100

Service Credit

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.95%	10%

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99%	25%

Additional Terms: Service Credits are applicable only to fees attributable to your use of Web Apps, Mobile Apps, API apps or Logic Apps and not to fees attributable to other types of apps available through the App Service, which are not covered by this SLA.

8.11 Data Disposal

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

Microsoft uses industry standard processes to delete Customer Data when it is no longer needed. Microsoft does not use customer data in non-production environments. In addition, Microsoft uses best practice procedures and a media wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. Microsoft Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.

Internal to CodeLynx: when information is determined to be no longer of use (during or at the end of the contract) the security team and project management representatives will request guidance for the disposition of the information. Client information will be returned as directed by the cognizant authority to the designated point of contact in the format specified. If directed, CodeLynx will delete and/or destroy using a client approved method that prevents its unauthorized disclosure within 48 hours. Methods for paper-based material includes crosscut shredding, burning, wet pulping, & chemical decomposition. Methods for electronic media include overwriting, degaussing, sanding, and physical destruction. Destruction will be witnessed and attested to by a member of the security team.

Azure follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.

8.12 Performance Measures and Reporting

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

CodeLynx response:

As all CodeLynx offerings fall under Microsoft Azure's SLA, reliability and uptime is guaranteed at a minimum of 99.9%, with many offerings maintaining 99.95% or 99.99%.

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

CodeLynx Response:

Guarantees vary by solution and service licensed. Please see Microsoft's SLAs for details about guarantees for specific proposed solutions. For complete details regarding Microsoft Azure Product Service Level Agreements, please visit https://azure.microsoft.com/en-us/support/legal/sla/

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

CodeLynx Response:

The first point of contact for any CodeLynx-related support issues will be the Purchasing Entity's dedicated Account Manager. They will be available to be contacted directly at their phone extension or at their CodeLynx email address. Depending on the type of support needed, the CodeLynx Account Manager will engage with appropriate resources to resolve the issue. For example, if the support needed is pre-sales technical support, our dedicated Microsoft Azure technical specialists will be available to answer questions via coordination from the CodeLynx Account Manager. If the support is more technical in nature the account manager will engage with the appropriate resources within Microsoft. If the support issue requires the Purchasing Entity to open a formal case/ticket with the Microsoft Azure Support team, the Purchasing Entity will need to submit the ticket/case directly with Microsoft.

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

CodeLynx Response:

To the extent that downtime results due to a service incident that is within the scope of Microsoft's standard SLA terms, those standard terms would provide a remedy based upon the amount of downtime.

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

CodeLynx Response:

CodeLynx schedules for planned downtime are flexible and will be determined in conjunction with the Purchasing Entity to minimize any inconvenience. In the event of Microsoft Azure resources require planned downtime, account administrators will be notified by e-mail as soon as possible.

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

CodeLynx Response:

If Microsoft does not achieve and maintain the Service Levels for each Service as described in an applicable SLA, then Purchasing Entities may be eligible for a credit towards a portion of their monthly service fees. Microsoft will not modify the terms of SLA during the initial term of the Purchasing Entities' subscription;

however, if Purchasing Entities renew their subscription, the version of this SLA that is current at the time of renewal will apply throughout the renewal term. We will provide at least 90 days' notice for adverse material changes to the SLA.

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

CodeLynx Response:

Microsoft Azure status and performance reports are available over the Web via the following link: https://azure.microsoft.com/en-us/status.

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

CodeLynx Response:

Historical, statistical, and usage reports are configurable and available in both Microsoft Azure and Microsoft Azure Government's account management portals/consoles.

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

CodeLynx Response:

All paid-for, on-demand deployments are supported 24x365. Free versions or limited trials may be subject to alternative terms and conditions, including support.

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

CodeLynx Response:

Customers may scale-up or scale-down all paid-for on-demand services 24x365. Free versions or limited trials may be subject to alternative terms and conditions, including support.

8.13 Cloud Security Alliance

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

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

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

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

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

Microsoft Azure and Microsoft Intune have been awarded CSA STAR Attestation. STAR Attestation provides an auditor's findings on the design suitability and operating effectiveness of SOC 2 controls in Microsoft cloud services.

Microsoft in-scope cloud services:

Azure and Azure Government

Azure Germany detailed list

Cloud App Security

Graph

Intune

Microsoft Flow cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite

PowerApps cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite

Power BI

Microsoft and CSA STAR Certification

Microsoft Azure, Microsoft Intune, and Microsoft Power BI have obtained STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture. This STAR certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It demonstrates that a cloud service provider conforms to the applicable requirements of ISO/IEC 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

During the assessment, an accredited CSA certification auditor assigns a Maturity Capability score to each of the 16 CCM control areas. The average score is then used to assign the overall level of maturity and the corresponding Bronze, Silver, or Gold award. Azure, Intune, Power BI, and Microsoft Cloud App Security were awarded Cloud Security Alliance (CSA) STAR Certification at the Gold level.

Microsoft and CSA STAR Self-Assessment

As part of the STAR Self-Assessment, CSPs can submit two different types of documents to indicate their compliance with CSA best practices: a completed CAIQ, or a report documenting compliance with CCM. For the CSA STAR Self-Assessment, Microsoft publishes both a CAIQ and a CCM-based report for Microsoft Azure, and CCM-based reports for Microsoft Dynamics 365 and Microsoft Office 365.

8.14 Service Provisioning

8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

CodeLynx has an expedited order processing facility that can escalate the internal order processing to move an emergency or rush order to the front of the queue and start it working immediately. This has been actioned in the past for state and local entities before and immediately after natural disasters. CodeLynx has also worked with State agencies to incorporate language into contracts and participating addenda to facilitate this type of emergency response facility including dedicated points of contact with 24/7 contact information provided to the State or agency. Once a customer's subscription is initiated, the customer can spin up Azure services on-demand, any time, through the customer's Administrative Console.

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

For product recommendations, quotes, and other requests, Eligible Entities can reach out to their CodeLynx Account Manager via phone, email, or fax. This information is displayed for each Eligible Entity on their CodeLynx Account Center site, once logged in. Account Managers' response to communication will be from 30 minutes to 2 business hours.

Whenever an Account Manager is out of the office, they designate a fellow coworker to assist their customers, so there is no gap in support. This designated backup will be Account Manager that supports other Eligible Entities, to ensure they are knowledgeable of the contract requirements.

8.15 Back Up and Disaster Plan

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

Business Continuity Plans (BCPs) have been documented and published for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum. The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.

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

Microsoft Azure has a number of features to make an application redundant at every level of failure, from an individual VM to an entire region.

Single VM. Azure provides an uptime SLA for single VMs. Although you can get a higher SLA by running two or more VMs, a single VM may be reliable enough for some workloads. For production workloads, we recommend using two or more VMs for redundancy.

Availability sets. To protect against localized hardware failures, such as a disk or network switch failing, deploy two or more VMs in an availability set. An availability set consists of two or more fault domains that share a common power source and network switch. VMs in an availability set are distributed across the fault domains, so if a hardware failure affects one fault domain, network traffic can still be routed the VMs in the other fault domains.

Availability zones. An Availability Zone is a physically separate zone within an Azure region. Each Availability Zone has a distinct power source, network, and cooling. Deploying VMs across availability zones helps to protect an application against datacenter-wide failures.

Paired regions. To protect an application against a regional outage, you can deploy the application across multiple regions, using Azure Traffic Manager to distribute internet traffic to the different regions. Each Azure region is paired with another region. Together, these form a regional pair. Except for Brazil South, regional pairs are located within the same geography in order to meet data residency requirements for tax and law enforcement jurisdiction purposes.

When you design a multi-region application, consider that network latency across regions is higher than within a region. For example, if you are replicating a database to enable failover, use synchronous data replication within a region, but asynchronous data replication across regions.

	Availability Set	Availability Zone	Paired region
Scope of failure	Rack	Datacenter	Region
Request routing	Load Balancer	Cross-zone Load Balancer	Traffic Manager
Network latency	Very low	Low	Mid to high
Virtual network	VNet	VNet	Cross-region VNet peering

Site Recovery & Backup Services

Customers have the option to utilize the Azure Site Recovery service to mitigate disasters.

Site Recovery service: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again.

Backup service: The Azure Backup service keeps your data safe and recoverable by backing it up to Azure. in, you can fail back to it.

Site Recovery can manage replication for:

Azure VMs replicating between Azure regions.

On-premises VMs and physical servers replicating to Azure, or to a secondary site.

Site Recovery provides the following features: business continuity disaster recovery (BCDR) solutions, Azure VM replication, on-premises VM replication, workload replication, data resilience, RTO and RPO targets, keeping apps consistent during failover, testing without disruption, flexible failovers, customized recovery plans, BCDR integration, Azure automation integration, and network integration.

The following items can be replicated:

Azure VMs from one Azure region to another

On-premises VMware VM, Hyper-V VMs, physical servers (Windows and Linux) to Azure

On-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site.

Customers should consider the region that they desire to failover to as not all regions offer every single product. There are 52 regions and the extensive list of products supported in each region can be found at: https://azure.microsoft.com/en-us/global-infrastructure/services/

Azure runs in geographically distributed Microsoft facilities, in some cases sharing space and utilities with other Microsoft Online Services (paired datacenters are located at least 300 miles apart to provide failover in the event of a large-scale regional disaster). Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel. Microsoft Azure also provides multiple mechanisms for customers to deploy fault-tolerance within their Azure subscription environment, including the configuration of failover clusters, geo-redundant storage, and load balancing.

The locations of Microsoft datacenters are chosen based on multiple criteria, which includes mitigation of environmental risks. In areas where there exists a higher probability of earthquakes, seismic bracing of the facility is employed. Environmental controls have been implemented to protect systems inside the facility, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

A single hardware failure is mitigated by a Fabric Controller which manages resource allocation, automatically failing-over to a different machine or cluster. Hardware management is transparent to the customer. Without additional configuration, data is protected by locally redundant storage, which maintains multiple replicas of data within a single region. If geo-replication for the virtual machine is configured, that geo-replication provides redundancy of data across regions to help ensure access to data in the event of a local disaster. Network infrastructure and components are similarly redundant, with N+1 links to regional TelCos, load balancers, and routing switch fabric.

Microsoft Azure employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, network backbone, Internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause. Azure Services teams continuously invest effort in developing greater application resiliency within software components, so they will quickly recognize a disruption and gracefully fail over to a different set of servers or even a different datacenter, without interrupting the availability of the service. Azure datacenters have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators, and datacenters have arrangements for emergency fuel delivery. Datacenters also have a dedicated Facility Operations Center to monitor the following: Power systems, including critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.

Azure conducts a risk assessment to identify and assess continuity risks related to Microsoft Azure services. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations. Business Impact Assessment, Dependency Analysis and Risk Assessments

are performed /updated at least on an annual basis. Customers are responsible for performing impact analysis for their applications and design to meet their Recovery Time Objective (RTO) / Recovery Point Objective requirements.

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

Azure currently maintains 52 regions worldwide that are available in 140 countries. In North America alone there are the East US, East US 2, Central US, North Central US, South Central US, West Central US, West US, West US 2, Canada East, Canada Central, and two undisclosed government locations.

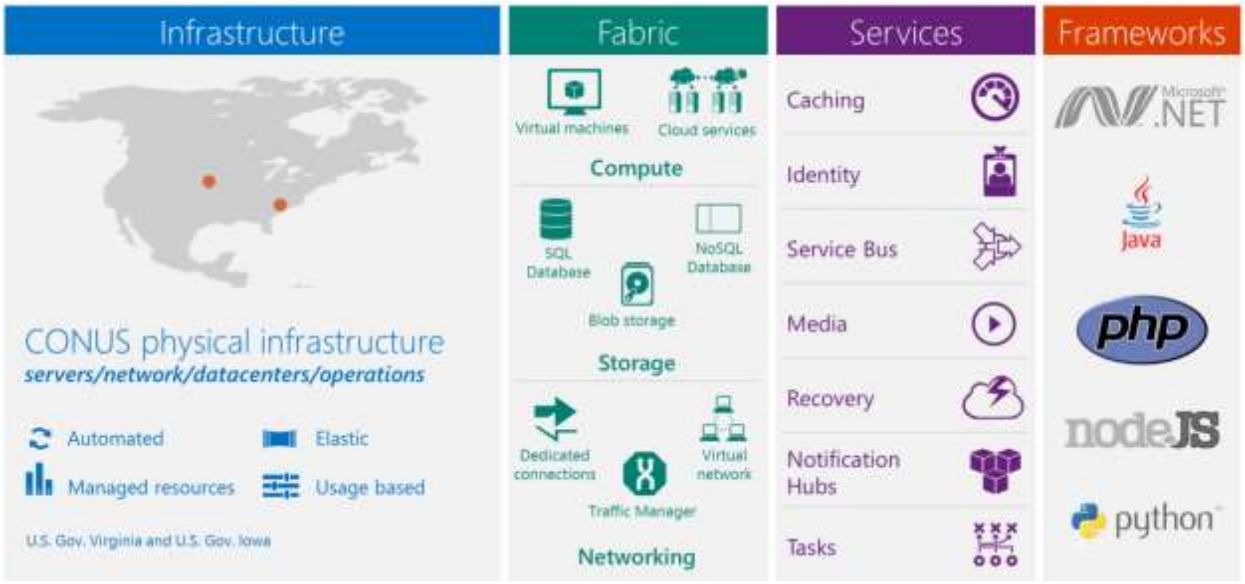
https://azure.microsoft.com/en-us/global-infrastructure/regions/

Each region contains a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. Customers have the option to select which region is right for them based off proximity to their location and/or the available services for that region. Further, regions are grouped into Geographies that may have different compliance standards in each location.

Azure provides high availability by offering protection from datacenter failure by utilizing Availability Zones. Each zone is a unique physical location with independent power, network, and cooling. Each zone is comprised of one or more datacenters and houses infrastructure to support highly available, mission critical applications. Availability zones are tolerant to datacenter failures through redundancy and logical isolation of services.

Azure Government offerings deliver a United States based cloud solution designed specifically to support strategic scenarios for U.S. government organizations including the Department of Defense, federal, state, and local governments, and their solution providers. It provides a comprehensive and open Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) for the U.S. government community including infrastructure, network, storage, data management and identity management delivered through secure and compliant hybrid cloud solution.

Azure Government core components include Compute, Storage, Networking, Identity and SQL database. Below is a diagram depicting the core capabilities that are delivered by Azure Government for IaaS and PaaS and will be discussed in detail below.



Azure Government was designed with the principles outlined below to help government organizations embrace cloud services. The key principles are:

Ease of Use - Make it easy for developers, system administrators, and architects to build, migrate, deploy, and manage applications, and lets you accelerate provisioning of resources to minutes instead of days or months.

Open and Flexible – Empower developers to choose the framework, tools, operating system and architecture to best meet their needs to build cloud solutions including .NET, Java, PHP and Node.js.

Secure and Compliant – Ensure Azure Government is using Microsoft Azure's world class security, compliance, and controls and is leveraging datacenters in the Continental U.S. (CONUS), screened U.S. personnel and policies to meet the higher level demands of US public sector customers.

Enterprise Ready- Provides enormous scalability, reliability, and use of common management and identity tools that enables hybrid cloud solutions to quickly build, migrate, deploy, and manage, reliable and scalable applications using existing IT environments.

When organizations combine the core Azure Government services above with these principles, it enables them to implement relevant scenarios and capture the benefits of the cloud. In the Azure Government

features section, we will break down the core components to help you understand the core services and then discuss some common workloads.

Azure Government provides a breadth of capabilities and services including infrastructure, fabric, services, and the frameworks that can be used to develop applications.

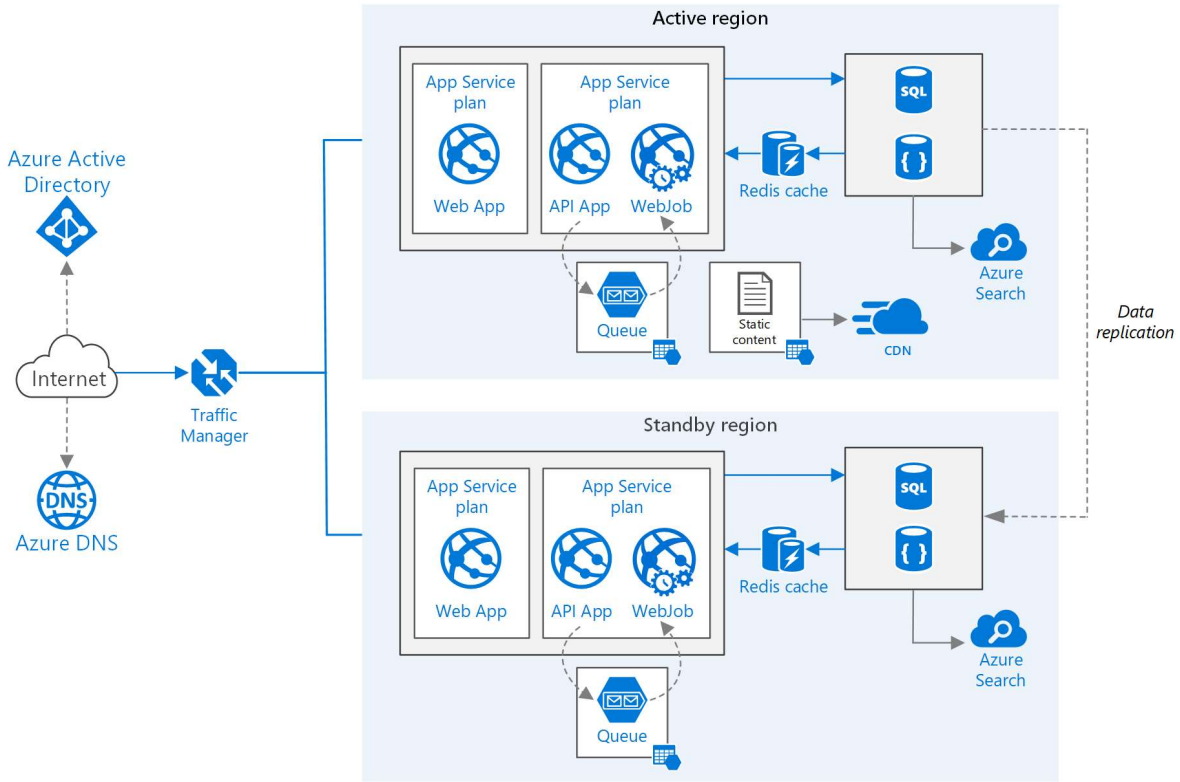
Its core capabilities include IaaS and PaaS which provides a rich set of compute, network infrastructure, storage, and identity management services. These provide government organizations the flexibility to choose either approach to quickly build, test, deploy, and manage applications. All government customer data, applications, and hardware reside in the Continental United States (CONUS) and are operated by screened U.S. Citizens.

8.16 Hosting and Provisioning

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

All provisioning is done by default using a web-based Management Portal, or Azure Resource Manager, or PowerShell commandlets, or an API using one of the provided SDKs (in JSON, REST, Node.js, PHP, Python, or Java). Additional provisioning stacks include Chef/Puppet (available as a native add-in and select third-party tools available in the Azure Marketplace.

Due to the wide variety of offerings from Microsoft Azure Government and Commercial and the variation of each client's unique necessities there are far too many provisioning processes to list in a single document. As such, CodeLynx offers a sample defined/standard provisioning stack for multi-region web application.



Customers may initiate a virtual machine utilizing IaaS with the intent on hosting a SQL server database which is far from the process of initiating a SaaS Office 365 subscription. Microsoft offers a plethora of guides for provisioning each type of service and the best practices for doing so.

8.16.2 Provide tool sets at minimum for:

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

2. Creating and storing server images for future multiple deployments

3. Securing additional storage space

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

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

Microsoft: By default this is accomplished using a web-based Management Portal, or Azure Resource Manager, or PowerShell commandlets, or an API using one of the provided SDKs (in JSON, REST, Node,js, PHP, Python, or Java).

2. Creating and storing server images for future multiple deployments

Microsoft: By default this is accomplished using a web-based Management Portal, or Azure Resource Manager, or PowerShell commandlets, or an API using one of the provided SDKs (in JSON, REST, Node,js, PHP, Python, or Java).

3. Securing additional storage space

Microsoft: By default this is accomplished using a web-based Management Portal, or Azure Resource Manager, or PowerShell commandlets, or an API using one of the provided SDKs (in JSON, REST, Node,js, PHP, Python, or Java).

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

Microsoft: Monitoring provides the granular usage statistics for every service in Azure. Billing and financial consumption is limited to the Account Owner. Resource and Service usage is available either in the Management Portal or via an API. Alerting and Response Management are provided by various services within Azure.

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

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

Microsoft, currently, as of the date of the Proposal, has a mechanism by which 30-day Trial subscriptions may be ordered for some, but not all, of the cloud services offered within this response. The Purchasing Entity may use this trial period of 30 days to test offerings or receive training on offerings.

The Purchasing Entity may purchase a separate subscription for establishing a second environment for testing or training purposes. Such separate subscription would be at an additional cost, and additional contract paperwork may be required.

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

Microsoft, currently, as of the date of the Proposal, has a mechanism by which 30-day Trial subscriptions may be ordered for some, but not all, of the cloud services offered within this response. The Purchasing Entity may use this trial period of 30 days to test offerings or proof of concept environment.

The Purchasing Entity may purchase a separate subscription for establishing a second environment for testing or proof of concept purposes. Such separate subscription would be at an additional cost, and additional contract paperwork may be required.

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

CodeLynx offers support related to authentication and account setup in the environment within the first 2 weeks of contract completion at no additional cost.

CodeLynx offers 4 hours of video conference enabled training at no additional cost upon completion of a contract.

8.18 Integration and Customization

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

CodeLynx will assist customers in choosing the right services and assist with the integration of those services in the customer's existing environment within the scope of this proposal. We will help customer enhance security and/or meet more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection/prevention and encryption.

Microsoft Cloud Solutions are specifically designed to support third-party technologies and were built with standards-based interfaces to enable integrations with these non-Microsoft tools. Many of these third-party technologies were built to run on Microsoft Windows platforms in the first place. Windows in the Azure Cloud and in Office 365 is the same as the Windows that these technologies were designed for. Microsoft even makes previous versions of Windows and SQL Server available in Azure, so that older applications that were designed for these previous versions can run in Azure as well.

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

Microsoft: Microsoft technology has always been developed with the end user in mind, so Microsoft Cloud Solutions are highly customizable and easily adaptable to the needs of the end user or their organization. Whether the Purchasing Entities want a SaaS, PaaS or IaaS solution, whether they want all or part of their business productivity tools in the Cloud, and whether they want to access it using Windows PCs or iOS devices, Microsoft Cloud Solutions are available. Purchasing Entities have a great deal of choice in the size, speed and performance level of all Cloud services they deploy and have several options for business productivity tools as well. Additionally, Microsoft is adding new options, new services, and new features every month.

8.19 Marketing Plan

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

CodeLynx currently has Cooperative Purchasing Contracts and Government Wide Acquisition Contract Schedules such as the GSA Schedule 70, the NASPO ValuePoint for Security and Fire Protection and other Statewide contracts. We intend to market and promote this NASPO contract in a similar manner to the way we have done with existing contracts. CodeLynx is an active participant, speaker, and exhibitor for government agency events such as the NASPO Exchange, NIGP State level and National events as well as other state, regional and national events. CodeLynx also participates in industry conferences and trade shows, holds open houses and road show type events to educate the end-users about the technologies and services available via these contracts. We have specifically held Azure boot camps in our offices and recorded the content in order to make it available to potential users. In addition, Microsoft provides numerous marketing channels, events and programs to assist us in connecting with users. We combine an on-line marketing outreach approach with person-to-person face time to earn the confidence and faith of our prospective clients and users.

8.20 Related Value-Added Services to Cloud Solutions

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

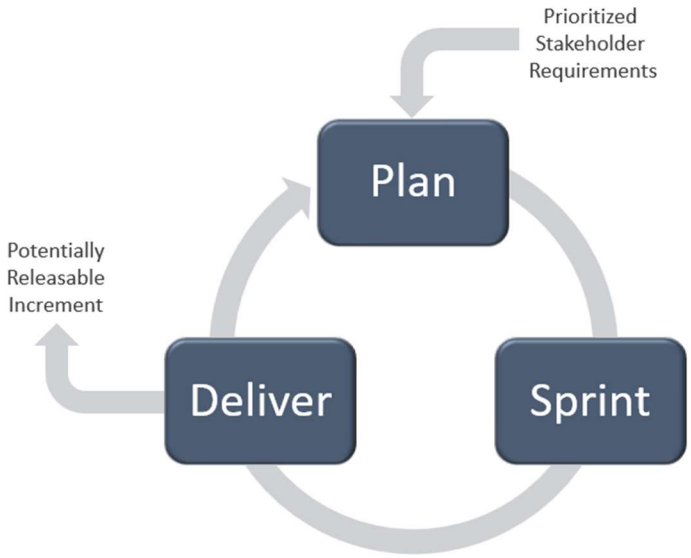
CodeLynx Response:

CodeLynx has extensive experience in full life cycle development applying the best industry practices and utilizes an Agile development approach to provide incremental functionality and to ensure that the product meets the needs and functional requirements of the stakeholders. We offer Project Management, training, and help desk support to all our clients, and customize each contract to fit their specific needs. As part of our project management methodology, clients will receive pre- and post-implementation consulting services to analyze their systems and make suggestions on the solution to ensure all requirements are met.

CodeLynx Agile Methodology

CodeLynx executes projects using an agile approach through the Scrum framework to foster collaboration and deliver high-value products to customers. This means we apply an iterative, incremental process that gives you unique opportunities for collaboration and acceptance of project components. Requirements and solutions are continuously evolving based on stakeholder feedback throughout the duration of the project.

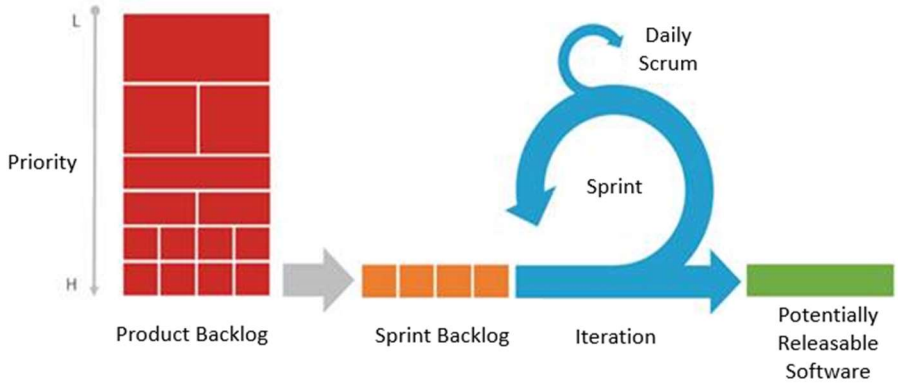
Each iteration cycles through the steps of Plan – Sprint – Deliver. At the end of each iteration, a potentially releasable project increment is demonstrated and reviewed with the client for feedback or acceptance. The benefit of the Scrum Framework is that no feature is considered complete until the client is satisfied with its implementation.



Project Initiation

CodeLynx will collaborate with the client and Product Owner to identify the needs of all users and to outline high-level requirements that satisfy their goals. We know how important it is for our clients to have effective and efficient tools to meet the demands of growing workloads and the cruciality of secure data in reliable cloud solutions. During project initiation, we will hold discovery sessions with the client and available stakeholders to document needs and define requirements.

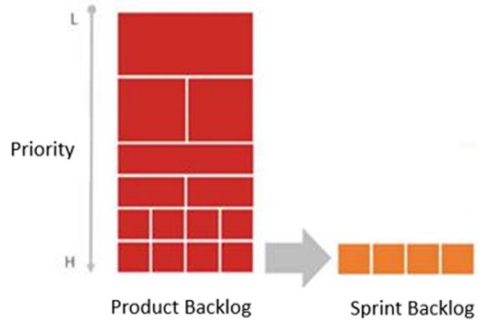
CodeLynx will use these high-level requirements to build the product backlog. The product backlog will evolve and become more detailed as the project progresses. The client prioritizes the work items in the backlog according to what will bring the highest value to the project. The CodeLynx Scrum Master will assist in determining the highest value items and ensure these items are implemented first.



Plan

As the business environment and other frameworks evolve, the clients' needs may change. The CodeLynx Scrum Master holds weekly sprint planning meetings during which client representatives and Product

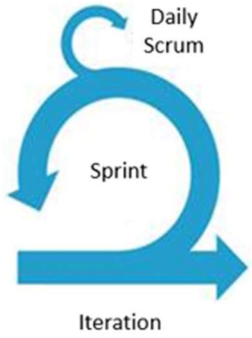
Owner will review the product backlog and update the priority of work items. The development team analyzes the highest priority work items for task breakdown. Approved requirements and designs are broken down into detailed tasks and placed in the sprint backlog for implementation in the upcoming sprint.



Sprint

Our team works in one to two-week sprints or work cycles depending on the needs of our clients and their current Scrum (or other development) processes. All work items that are placed in the sprint backlog during the sprint planning meeting are created, reviewed, and thoroughly tested by the CodeLynx Scrum Master, development team, and Quality Assurance Analyst. The team is committed to getting the product increment to a state of "Done" so that it can be demonstrated and potentially released.

The CodeLynx Scrum Master facilitates the Daily Scrum for the CodeLynx team every morning to ensure the project is on-track or remove any impediments the team may have.



Deliver

The releasable items completed in each sprint are demonstrated and reviewed with the client for feedback during sprint review meetings. The purpose of this review is to analyze the completed increment and verify requirements are satisfied. Necessary modifications are documented, and the product backlog is updated to add detail to the high-priority work items. The process of Plan – Sprint – Deliver starts over for the project's next iteration.

Once the solution is accepted, a Go Live date will be set. CodeLynx will support the "Go Live" event as needed. Following a successful Go Live, we will move into the Maintenance period if contracted by the client.

Training Support

CodeLynx has extensive experience in providing relevant and effective training and training materials for cloud solutions, including quick reference guides and training exercises created by our technical writing team. We also provide excellent training both in-person and online. After meeting with end users and assessing the training needs of the client, CodeLynx will develop appropriately detailed training material and update the training plan to ensure all learning types and technological literacy levels are considered.

8.21 Supporting Infrastructure

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

The infrastructure requirements will vary based upon which service the purchasing entity wants, the number of users, and the intended use. In most cases there will be little to no infrastructure required for a particular solution. In cases where a hybrid cloud solution is desired, CodeLynx will need access to the on-premise infrastructure we will be integrating with the Azure cloud. Along the same lines if we are performing a migration from an on-premise solution to a cloud based solution CodeLynx will need access to the on-premise infrastructure.

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

For Microsoft cloud services, it will be the purchasing entity's responsibility to install any new infrastructure required at their site, and they will be the ones incurring costs. CodeLynx has the resources to help with those installations, but networking, security, and end user devices, are not in scope of this contract.

Due to the extensive number of services offered by Microsoft Azure and the fact that each service has its own Service Level Agreements (SLAs) the following URLs are provided that summarizes each service's SLA and provides links to each service's SLA. As well as the subscription agreements or EULAs for the commercial and government enclaves.

SLA summary for Azure Services

https://azure.microsoft.com/en-us/support/legal/sla/summary/

Microsoft Online Subscription Agreement

https://azure.microsoft.com/en-us/support/legal/subscription-agreement/

Microsoft Online Subscription Agreement – US Government Cloud

https://azure.microsoft.com/en-us/support/legal/subscription-agreement/government/