STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 1

CONTRACT #: AR3107

Starting Date: 11/8/2019

Expiration Date: 9/15/2026

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and International Business Machines Corp (IBM Corporation) (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

Amend the Master Agreement AR3107 and add the language in accordance with attachment below "Amendment 1 to the IBM NASPO Cloud Master Agreement"

Effective Date of Amendment: 7/1/2023

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

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

CONTRACTOR

Contractor's Signature — Date: 29 June 2023

Karen Schneider
Contractor's Name (Print)

NASPO Nat'l Pgm Mgr
Title (Print)

STATE OF UTAH

DocuSigned by:
C38BE9DAC528424...
Director, State of Utah Division of Purchasing — Date: 7/6/2023

For Division of Purchasing Internal Use

Purchasing Agent	Phone #	E-mail Address	Contract #
Blake Theo Porter	801-957-7136	btporter@utah.gov	AR3107

Amendment 1 to the IBM NASPO Cloud Master Agreement

International Business Machines Corporation's (IBM's) NASPO Cloud Solutions Master Agreement is amended as follows to (a) clarify IBM's ability to provide third-party Software-as-a-Service (SaaS) solutions; (b) utilize third-party data centers and infrastructure for delivering Cloud Services and Professional Services; and (c) provide stand-alone Professional Services in support of IBM or third-party SaaS and Platform-as-a-Service (PaaS) solutions.

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:

(i) A Participating Entity's Participating Addendum ("PA").

(ii) NASPO ValuePoint Master Agreement Terms & Conditions, including the following Exhibits:

(1) Exhibit 1: Software-as-a-Service

(2) Exhibit 2: Platform-as-a-Service

(3) Exhibit 3: Infrastructure-as-a-Service

(iii) IBM Ordering Documents (also known as Transaction Documents, or TDs), which shall incorporate the applicable hosting and delivery policies, IBM's Cloud Services Agreement (CSA), Data Processing Agreement (DPA) and Data Security and Privacy Principles for IBM Cloud Services (DSP), as well any other applicable service documentation. Copies of the IBM CSA, DPA, and DSP current as of the effective date of this Master Agreement, are attached hereto as Addendums 1 - 3. These documents may also be found at www.ibm.com/support/customer/csol/terms and at https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf. Online versions are for reference only, and the official versions for purposes of this Agreement and an Order are the ones posted to the NASPO ValuePoint website (https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/) or at such other site as agreed to by NASPO and IBM.

Any applicable Third-Party product license terms shall be included in the applicable Transaction Document corresponding to their purchase or use, including incorporated Third-Party data security terms.

The Lead State agrees that this Master Agreement and the information which is incorporated into this Master Agreement by written reference together with the

applicable Order and Participating Addendum, is the complete agreement for the Services ordered by the Purchasing Entity and supersedes all prior or contemporaneous agreements or representations, written or oral, regarding such Services.

It is expressly agreed that the documents in the order of precedence above shall supersede the terms in any purchase order, procurement internet portal, or other similar non-IBM (or non-Third-Party as offered or support by IBM) document and no terms included in any such purchase order, portal, or other non-IBM or non-Third-Party document shall apply to the Services ordered. In the event of any inconsistencies between the terms of an Order and the Master Agreement, the Master Agreement shall take precedence; however, unless expressly stated otherwise in an Order, the terms of the Data Processing Agreement and Data Security and Privacy Principles for IBM Cloud Services shall take precedence over the Order. No third party beneficiary relationships are created by this Master Agreement.

The parties agree to review any updates and or changes to the IBM documents in a timely manner.

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

Cloud Services means, collectively, the IBM or Third-Party cloud services (e.g., IBM/Third-Party software as a service offerings and related IBM/Third-Party Programs) listed in Purchasing Entity's Order and defined in the Service Specifications. The term "Cloud Services" does not include Professional Services.

Professional Services means, collectively, the Cloud Services-related consulting and other professional services which Purchasing Entity has ordered. Professional Services include any deliverables described in Purchasing Entity's Order and delivered by IBM to Purchasing Entity under the Order. The term "Professional Services" does not include Cloud Services. Professional Services may be acquired independently of Cloud Services and support either IBM Cloud Services or a Third-Party Cloud Services, independent of whether Purchasing Entity acquired such Cloud Services from IBM or from Third-Parties.

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 or Third-Party's applications running on a Contractor's or Third-Party'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.

Third-Party refers to entities independent of Contractor whose Cloud Services are offered by Contractor or supported by a Contractor Professional Service.

Third-Party Programs refers to the software products owned or licensed by a Third-Party to which IBM grants Purchasing Entity access as part of the Cloud Services, including Program Documentation, and any program updates provided as part of the Cloud Services.

23. Operations Management: Contractor or Third-Party 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 those specified in the Solicitation

44. Additional Terms and Conditions

***

c. Use of Services:

***

iii. The Purchasing Entity is required to accept all patches, bug fixes, updates, maintenance and service packs (collectively, "Patches") necessary for the proper function and security of the Services, including for the IBM and/or Third-Party Programs, as such Patches are generally released by IBM and/or Third-Parties as described in the Service Specifications. IBM is not responsible for performance or security issues encountered with the Cloud Services that result from the Purchasing Entity's failure to accept the application of Patches that are necessary for the proper function and security of the Services. Except for emergency or security related maintenance activities, IBM will coordinate with the Purchasing Entity the scheduling of application of Patches, where possible, based on IBM's or Third-Party's next available standard maintenance window.

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

3. **Data Location:** As selected by Purchasing Entity from available Contractor and/or Third-Party data centers, the Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S and 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 U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical and general administrative 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.

8. Background Checks:

a. Contractor follows a mandated set of employment verification requirements for all new hires, including regular, fixed term, supplementals, part time, interns, early professional and professional hires. These standards apply to Contractor's wholly owned subsidiaries and joint ventures. They do not apply to Third-Parties providing platforms/infrastructure/software that do not have access to Purchasing Entity's data. The requirements currently include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each country is responsible for implementing the above requirements in their hiring process as applicable and permissible pursuant to each country's local laws.

When requested under an applicable TD, the Contractor shall conduct a background investigation in accordance with Contractor's internal process. This investigation may be at the Purchasing Entity's expense. Contractor will conduct the background and/or verification checks in accordance with Contractor's polices and applicable law and background report may include a check of a national criminal database as well as the OFAC Listing.

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

c. If any of the stated personnel providing services under an applicable TD is not acceptable to the Purchasing Entity as a result of the background investigation, the Purchasing Entity, shall have the option to either (1) request replacement of the person, or (2) terminate the Participating Addendum and any related service agreement in accordance with the Termination Section of the Master Agreement.

11. Data Center Audit: The Contractor shall only be responsible for performing an independent audit of its data centers at least annually at its expense, and upon request to a Purchasing Entity with a written non-disclosure agreement. A redacted Service Organization Control (SOC) 2 audit report or equivalent third-party audit will be provided. Data Center audit reports are Confidential Information of Contractor and shall be treated as such at all times. Access to such reports under an Open Records or Freedom of Information Act provision shall be addressed as needed in the Participating Addendum under which a Purchasing Entity procures a Cloud Service. Physical access to data centers is prohibited except as required by law. Any independent audit of Third-Party data centers used to deliver PaaS under this Agreement shall be completed by the Third-Party and provided to client in the same manner as described above.

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

3. Data Location: As selected by Purchasing Entity from available Contractor and/or Third-Party data centers, the Contractor shall provide its services to the Purchasing Entity and its end users solely from Contractor and/or Third-Party 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 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.

8. Background Checks:

a. Contractor follows a mandated set of employment verification requirements for all new hires, including regular, fixed term, supplementals, part time, interns, early professional and professional hires. These standards apply to Contractor's wholly owned subsidiaries and joint ventures. They do not apply to Third-Parties providing platforms/infrastructure/software that do not have access to Purchasing Entity's data. The requirements currently include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each country is responsible for implementing the above requirements in their hiring process as applicable and permissible pursuant to each country's local laws.

When requested under an applicable TD, the Contractor shall conduct a background investigation in accordance with Contractor's internal process. This investigation may be at the Purchasing Entity's expense. Contractor will conduct the background and/or verification checks in accordance with Contractor's polices and applicable law and background report may include a check of a national criminal database as well as the OFAC Listing.

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

c. If any of the stated personnel providing services under an applicable TD is not acceptable to the Purchasing Entity as a result of the background investigation, the Purchasing Entity, shall have the option to either (1) request replacement of the person, or (2) terminate the Participating Addendum and any related service agreement in accordance with the Termination Section of the Master Agreement.

11. Data Center Audit: The Contractor shall only be responsible for performing an independent audit of its data centers at least annually at its expense, and upon request to a Purchasing Entity with a written non-disclosure agreement. A redacted Service Organization Control (SOC) 2 audit report or equivalent third-party audit will be provided. Data Center audit reports are Confidential Information of Contractor and shall be treated as such at all times. Access to such reports under an Open Records or Freedom of Information Act provision shall be addressed as needed in the Participating Addendum under which a Purchasing Entity procures a Cloud Service. Physical access to data centers is prohibited except as required by law. Any independent audit of Third-Party data centers used to deliver SaaS under this Agreement shall be completed by the Third-Party and provided to client in the same manner as described above.

All other terms and conditions of the NASPO Cloud Master Agreement shall continue to apply.

Contract #: AR3107

STATE OF UTAH COOPERATIVE CONTRACT

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

International Business Machines Corp
Name

7100 Highlands Parkway
Street Address

Smyrna	GA	30082
City	*State*	*Zip*

Vendor # 94833A Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact *Name:* Karen Schneider *Phone Number:* 720-397-5563 *Email:* kasch@us.ibm.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, November 08, 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
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs

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

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

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

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

CONTRACTOR

Karen Schneider (Nov 13, 2019) — Nov 13, 2019
Contractor's signature — Date

Karen Schneider — Nov 13, 2019
Type or Print Name and Title

DIVISION OF PURCHASING

Nov 13, 2019
Director, Division of Purchasing — Date

Note: Sections negotiated 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33, 35, 36, 40, 41, 42, 43, 44, & 46.

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:

(i) A Participating Entity's Participating Addendum ("PA") [1].

(ii) NASPO ValuePoint Master Agreement Terms & Conditions, including the following Exhibits: [2]

(1) Exhibit 1: Software-as-a-Service

(2) Exhibit 2: Platform-as-a-Service

(3) Exhibit 3: Infrastructure-as-a-Service

(iii) IBM Ordering Documents (also known as Transaction Documents, or TDs), which shall incorporate the applicable hosting and delivery policies, IBM's Cloud Services Agreement (CSA), Data Processing Agreement (DPA) and Data Security and Privacy Principles for IBM Cloud Services (DSP), as well any other applicable service documentation. Copies of the IBM CSA, DPA, and DSP current as of the effective date of this Master Agreement, are attached hereto as Addendums 1 - 3. These documents may also be found at www.ibm.com/support/customer/csol/terms and at https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf. Online versions are for reference only, and the official versions for purposes of this Agreement and an Order are the ones posted to the NASPO ValuePoint website (https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/) or at such other site as agreed to by NASPO and IBM.

The Lead State agrees that this Master Agreement and the information which is incorporated into this Master Agreement by written reference together with the applicable Order and Participating Addendum, is the complete agreement for the Services ordered by the Purchasing Entity and supersedes all prior or contemporaneous agreements or representations, written or oral, regarding such Services.

It is expressly agreed that the documents in the order of precedence above shall supersede the terms in any purchase order, procurement internet portal, or other similar non-IBM

[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.

document and no terms included in any such purchase order, portal, or other non-IBM document shall apply to the Services ordered. In the event of any inconsistencies between the terms of an Order and the Master Agreement, the Master Agreement shall take precedence; however, unless expressly stated otherwise in an Order, the terms of the Data Processing Agreement and Data Security and Privacy Principles for IBM Cloud Services shall take precedence over the Order. No third party beneficiary relationships are created by this Master Agreement.

The parties agree to review any updates and or changes to the IBM documents in a timely manner.

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

Ancillary Software means any software agent or tool that IBM makes available to the Purchasing Entity for download for purposes of facilitating the Purchasing Entity's access to, operation of, and/or use with, the Services Environment.

Cloud Services means, collectively, the IBM cloud services (e.g., IBM software as a service offerings and related IBM Programs) listed in Purchasing Entity's Order and defined in the Service Specifications. The term "Cloud Services" does not include Professional Services.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential, that is disclosed or otherwise made available in the performance of this Master Agreement by either party to the other party, including by a Participating Entity or Purchasing Entity or each of theirrespective employees or agents, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals.

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 following the risk assessment process receiving a Data Categorization as "High Risk Data", Moderate Risk Data", or "Low Risk Data", whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, integrity or ability to access 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". For purposes of clarity, the categorization of the data is the responsibility of the Purchasing Entity.

Data Center Region refers to the geographic region in which the Services Environment is physically located. The Data Center Region applicable to the Cloud Services is set forth in the Purchasing Entity's Order.

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 remarketing requirements of 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.

IBM means International Business Machines Corporation, the Contractor.

IBM Programs refers to the software products owned or licensed by IBM to which IBM grants Purchasing Entity access as part of the Cloud Services, including Program Documentation, and any program updates provided as part of the Cloud Services.

Incident means an incident that creates suspicion of unauthorized access to or handling of Personal 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 of Utah.

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

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, together with Exhibit 1(Software-as-a-Service), Exhibit 2 (Platform-as-a-Service), and Exhibit 3 (Infrastructure-as-a-Service), each of which is attached hereto and incorporated herein, 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.

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. For purposes of clarity, it is the responsibility of the Purchasing Entity to inform Contractor of such classification.

Order or **Ordering Document** means the Contractor's or Contractor's authorized reseller's standard ordering document signed by Purchasing Entity when placing an order for Service pursuant to the Master Agreement.

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 Protected 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.

Professional Services means, collectively, the Cloud Services-related consulting and other professional services which Purchasing Entity has ordered. Professional Services include any deliverables described in Purchasing Entity's Order and delivered by IBM to Purchasing Entity under the Order. The term "Professional Services" does not include Cloud Services.

Program Documentation refers to the user manuals referenced within the Service Specifications for Cloud Services as well as any help windows and readme files for the IBM Programs that are accessible from within the Services. The Program Documentation describes technical and functional aspects of the IBM Programs. Purchasing Entity may access the documentation online at https: www.ibm.com/cloud or such other address specified by IBM.

Protected Health Information or (PHI). Protected Health Information, as defined at 45 C.F.R. § 160.103) that is subject to protection under the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996, as amended, including by the Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act of 2009 ("HITECH Act").

Purchasing Entity means a state, city, county, district, or 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 becoming financially committed to the purchase.

Purchasing Entity Applications means all software programs, including any source code for such programs, that the Purchasing Entity or the Purchasing Entity's Users provide and load onto, or creating using, any IBM "platform-as-a-service" or "infrastructure-as-a-service" Cloud Services. Services under this Master Agreement, including IBM Programs and Services Environments, IBM intellectual property, and all derivative works thereof, do not fall within the meaning of the term "Purchasing Entity Applications".

Purchasing Entity Content means all text, files, images, graphics, illustrations, information, data (including Personal Data as that term is defined in Data Processing Agreement for IBM Cloud Services attached as Addendum 2), audio, video, photographs and other content and material (other than Purchasing Entity Applications), in any format, provided by the Purchasing Entity or on behalf of the Purchasing Entity's Users that reside in, or run on or through the Services Environment.

Services mean any of the specifications described in the Scope of Services/SLA/SOW/SD/Ordering Document that are supplied or created by the Contractor pursuant to this Master Agreement. The following terms may be interchange under the Master Agreement and any applicable purchases or services provided there under, including but not limited to: Transaction Document (TD), Scope of Work (SOW), Statement of Work

(SOW), Service Description (SD), Change Order, Quote, Service Level Agreement (SLA), Order Document, Purchase Order (PO), Purchase Agreement, Order, Price Agreement, Service Order, Task Order (TO), and Work Order.

Security Breach for the specific purpose of handling an incident in the Data Processing Agreement means the misappropriation of Personal Data located on IBM systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such information.

Services Environment refers to the combination of hardware and software components owned, license, or managed by IBM to which IBM grants Purchasing Entity and Purchasing Entity's Users access as part of the Cloud Services which Purchasing Entity has ordered. As applicable and subject to the terms of this Master Agreement and Purchasing Entity's Order, IBM programs, Third Party Content, Purchasing Entity Content and Purchasing Entity Applications may be hosted in the Services Environment.

Service Specifications means the descriptions by IBM that are applicable to the Services under Purchasing Entity's Order, including not limited to any Program Documentation, data sheets, hosting, support and security policies (for example, IBM Cloud Services Agreement), and other descriptions referenced or incorporated in such descriptions or Purchasing Entity's Order.

Service Level Agreement (SLA) issued against a Participating Addendum 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. SLAs may also be included in a Statement of Work (SOW), Ordering Document (Order or PO) or Service Description (SD) depending on the Service offering purchased by the Purchasing Entity ("SLA/SOW/SD").

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 (SOW) and/or Service Description (SD) means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

Third Party Content means all text, files, images, graphics, illustrations, information, data, audio, video, photographs and other content and material, in any format, that are obtained or derived from third party sources outside of IBM and made available to Purchasing Entity through, within, or in conjunction with Purchasing Entity's use of, the Cloud Services. Examples of Third Party Content include data feeds from social network services, rss feeds from blog posts, and data libraries and dictionaries and marketing data.

Users mean those employees, contractors, and end users, as applicable, authorized by the Purchasing Entity or on the Purchasing Entity's behalf to use the Cloud Services in accordance with this Master Agreement and Purchasing Entity's Order. For Cloud Services that are specifically designed to allow the Purchasing Entity's clients, agents, customers, suppliers or other third parties to access the Cloud Services to interact with the Purchasing Entity, such third parties will be considered "Users" subject to the terms of this Master Agreement and Purchasing Entity's Order.

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 except as set forth in a Participating Addendum, e.g. ordering procedures specific to the Participating Entity, other terms and conditions, subject to approval of the individual state procurement director and compliance with local statutory and regulatory provisions.

5. Assignment/Subcontracts: Except in the event of a merger, consolidation, acquisition, internal restructuring, or sale of all or substantially all of the assets of IBM, 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 WSCA-NASPO Master Agreement Administrator. The Lead State may not assign the Master Agreement and no Participating Entity may assign its Participating Addendum, in whole or in part, without the prior approval of Contractor. No Purchasing Entity may give or transfer the Services ordered under an Ordering Document to another individual or entity. Assignment of IBM rights to receive payments is not restricted.

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 only net new Orders this Master Agreement in the event IBM's commercial list price for the Services decreases. A price or rate reduction reflected in IBM's commercial list price will apply automatically to the Master Agreement for purposes of net new Orders only, 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.

Any termination under this provision shall not affect the rights and obligations that survive termination or expiration of this Master Agreement, such as those relating to limitation of liability, indemnification, payment and others which by their nature are intended to survive.

Termination of the Master Agreement or any Participating Addendum will not affect Orders that are outstanding at the time of termination, as permitted in a Participating Entity's Participating Addendum. Those Orders will be performed according to their terms as if this Master Agreement or the Participating Addendum were still in full force and effect. However, those Orders may not be renewed subsequent to termination of this Master Agreement.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

b. Non-Disclosure. Each party shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, but no less that the standard of care such party uses for its own similar confidential information, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Each party shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Each party shall use commercially reasonable efforts to assist the disclosing party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, the receiving party shall advise the disclosing party (including, as applicable the Purchasing Entity, applicable Participating Entity, and the Lead State) immediately if the receiving party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and the receiving party shall at its expense cooperate with the disclosing party in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by the disclosing party, the receiving party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at the disclosing party's request, the receiving party shall turn over to the disclosing party all documents, papers, and other matter in the receiving party's possession that embody Confidential Information. If applicable law, regulation or

document retention policy prevents the receiving party from destroying or returning all or part of the Confidential Information, the receiving party shall maintain the security and confidentiality of all such retained Confidential Information. Notwithstanding the foregoing, the receiving party may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Each party acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information and that the disclosing party shall be entitled, without waiving any other rights or remedies under this Master Agreement, to seek such injunctive or equitable relief as may be deemed proper by a court of competition jurisdiction.

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 and any applicable statutory, local, or constitutional requirements. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with consent, may be included in the Ordering used by the Purchasing Entity to place the Order.

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.

IBM may orally refer to this Master Agreement, and the potential work and activities covered by this Master Agreement, and may orally reference the Lead State or a Participating Entity as a customer in sales presentations and activities.

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 material contractual requirements; or

(2) A material breach of any applicable 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 intentionally 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 expressly specified in another section of this Master Agreement.

b. Upon the occurrence of an event of material default, the non-breaching party shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days (or an additional period of time as may be agreed to by the parties) in which the other party shall have an opportunity to cure the default. Each party will allow the other a reasonable opportunity to comply before it claims that the other has not met its obligations under this Agreement or an Ordering Document. The parties will attempt in good faith to resolve all disputes, disagreements or claims relating to this Agreement or any Ordering Document. In the event of a Contractor default, the Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate either party's liability for damages.

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

(1) Exercise any remedy provided by law; and

(2) Terminate the applicable portions that are the subject of the material breach in the Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor's performance; and

(4) Withhold applicable payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, either party 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. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under this Master Agreement.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, consisting of Contract Manager & Report Administrator, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified above. 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 to this (i) Master Agreement, (ii) a participating Addendum, or (iii) an Ordering Document shall be in default by reason of any failure or delay 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, restrictive acts of the government (including the denial or cancelation of any export, import, or other license) 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. The parties will both use reasonable efforts to mitigate the effect of a force majeure event. If such event continues for more than 30 days, either party may cancel unperformed Services and affected Orders upon written notice. This Section does not excuse either party's obligation to take reasonable steps to follow its normal disaster recovery procedures or Purchasing Entity's obligation to pay for the Service.

13. Indemnification

a. Indemnification – Other than for Intellectual Property. The Contractor shall indemnify and hold harmless by defending (which includes paying fees and related costs of defense) 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 legally liable (each, an "Indemnified Party" and collectively, the "Indemnified Parties"), from and against applicable, defined third-party claims, damages or causes of action brought against an Indemnified Party, for any death, bodily injury, or damage to real or tangible personal property arising directly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, in the performance under the Master Agreement. As used in this Section 13(a), the term "tangible personal property" shall not include software, documentation, data or data files. Contractor shall have no liability for any claim of bodily injury and/or tangible personal property damage arising from use of software or hardware. **This Section 13(a) states Contractor's entire liability and an Indemnified Party's exclusive remedy for bodily injury and property damage.**

b. Indemnification – Intellectual Property.

1. The Contractor shall indemnify and hold harmless by defending (which includes paying fees and related costs of defense) an Indemnified Party, from and against applicable, defined third-party claims, damages or causes of action brought against an Indemnified Party, arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

2. The Contractor's obligations under this section shall not extend to any claims arising from, and Contractor has no responsibility for claims based on, (a) non-Contractor products and services, (b) items not provided by Contractor, or (c) any violation of law or third-party rights caused by Client's content, materials, designs, or

specifications.

3. The Contractor's obligations under this section shall not extend to any claims arising from, and Contractor has no responsibility for claims based on, the combination of the Product with any other product, system or method, regardless of if 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; (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. Contractor has no responsibility for claims based, in whole or part, on Non-Contractor Products, items not provided by Contractor, or any violation of law or third-party rights caused by Participating Entity's content, materials, designs, specifications, or use of a non-current version or release of a Contractor Product when an infringement claim could have been avoided by using a current version or release. Contractor reserves the right to modify or replace a Service with an equivalent non-infringing one or, if replacement is not reasonably available, to discontinue a Service and provide a credit for any pre-paid unexpired term. The Indemnified Parties are responsible for any violation of law or any third-party rights caused by its content or, except as provided in this paragraph, its use of a Service.

4. **This Section 13(b) provides the Indemnified Party's exclusive remedy for any infringement claims or damages.**

c. The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim or other indemnified claim or cause of action. Contractor will defend the Indemnified Party against such claims pursuant to this Section 13, and pay amounts finally awarded by a court against the Indemnified Party or included in a settlement approved by Contractor, provided that the Indemnified Party promptly (i) notifies Contractor in writing of the claim, (ii) supplies information requested by Contractor, and (iii) allows Contractor to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. This section is 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 its 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 its 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, 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/Cyberisk Liability including Professional 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

Nothing in this Master Agreement shall be deemed to preclude IBM from selecting a new insurance carrier or carriers or obtaining new or amended policies at any time, as long as the above insurance coverage is maintained. This provision is not intended to, and does not, increase or decrease IBM's liability under the Limitation of Liability provision of this Master Agreement.

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements. Contractor will carry Crime or Employee Fidelity Coverage for loss of money, securities and other tangible property belonging to the Participating Entity resulting directly from a fraudulent or dishonest act by a Contractor employee taken by any means including via a computer, while performing professional services for the Participating

Entity.

(4) Professional Errors and Omissions. As applicable, Professional Errors and Omissions 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 written notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor in accordance with the terms of the policy.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a Certificate of Insurance to the Contractor's Commercial General Liability insurance policy 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 in accordance with the terms of the policy 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 only with respect to liability arising out of this contract. 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 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 if applicable to the insurance policy: 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, insurance amounts, 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.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations that are applicable to IBM in its role as a provider of information technology products and services under this agreement. Each party is responsible for complying with: i) laws and regulations applicable to its business and content, and ii) import, export and economic sanction laws and regulations, including those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users. The Purchasing Entity is responsible for its use of Contractor and non-Contractor products and services.

18. No Waiver of Sovereign Immunity: The Lead State, Participating Entity or Purchasing Entity to the extent it applies, does not waive its sovereign immunity by entering into this Contract and fully retains all immunities and defenses provided by law with regard to any action based on this Contract. If a claim must be brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court of (a) a Participating Entity's State if the dispute is between a Participating Entity or Purchasing Entity of that State, and Contractor; or (b) the Lead State if the dispute involves the Lead State.

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 as appropriate.

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. If the Purchasing Entity provides the necessary information to Contractor, 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 an Ordering Document.

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. Communications concerning administration of Orders placed under this Master Agreement 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 attempted 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.

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. This shall not prohibit the Lead State or other interested Participating States from negotiating different terms and conditions in its Participating Addendum.

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

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement.

21. Charges, Taxes and 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 may be remitted by mail or electronically. Payments may be made via a State or political subdivision "Purchasing Card" with no

additional charge. Purchasing Entity agrees to pay all applicable charges specific for a Service by Contractor and charges for use in excess of authorizations. Charges are exclusive of applicable taxes, levies, or fees imposed by any governmental authority resulting from Purchasing Entity's acquisitions under this Master Agreement, and any late payment fees. Charges shall be identified on Contractor's invoice. Prepaid Services must be used within the applicable period. Contractor does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid.

22. Data Access Controls: Data Access Controls will be set forth and governing in the applicable Ordering/SOW/SLA/SD agreements which may include the following terms as agreed upon therein: 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 those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents, except Confidential or Protected Information, 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 Purchasing Entity's Protected Data provided by it. Except as allowed under the provisions herein or unless otherwise provided in a Statement of Work or Service Level Agreement applicable to this provision, Contractor shall not collect, access, or use user-specific Purchasing Entity Protected Data except as necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service will be used by the Contractor for personal gain or make any other improper use of such application information as 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 except if Protected Data is legally or contractually subject to application Statue of Limitation or Survival terms.

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 allow authorized agents of a government agency to audit financial data records, pertaining to this Master Agreement and orders placed by Purchasing Entities under it and its internal and external auditors once a year, subject to thirty (30) days prior written notice received by the Contractor, at a mutually agreed upon time during normal business hours, and in a manner that does not unreasonably disrupt Contractor's or customer's business and subject to Contractor's reasonable security and confidentiality requirements/procedures /policies. Contractor will assist 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, from whom Purchasing Entity will obtain a written agreement sufficient to obligate them to maintain the Contractor's Confidential Information in confidence in a manner not less protective than obligations under the Master Agreement Section 8 Confidentiality) in auditing only information (excluding costs) which is relevant to the provision of Services purchased under this Master Agreement. Contractor will provide access to information and data reasonably necessary to perform the audit. Contractor shall not allow Purchasing Entity or its auditor access to data of other Contractor customers, or except as necessary to comply with the foregoing, to Contractor's Confidential Information 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. Contractor may audit the Purchasing Entity's use of the Services (e.g., through use of software tools) to assess whether the Purchasing Entity's use of the Services is in accordance with the Purchasing Entity's Order and the terms of this Master Agreement. The Purchasing Entity agrees to cooperate with Contractor's audit and provide reasonable assistance and access to information. Any such audit shall not unreasonably interfere with the Purchasing Entity's normal business operations. The Purchasing Entity agrees to pay within 60 days of written notification any fees applicable to the Purchasing Entity's use of the Services in excess of the Purchasing Entity's rights. If the Purchasing Entity does not pay, Contractor can end the Purchasing Entity's Services and/or the Purchasing Entity's Order. The Purchasing Entity agrees that Contractor shall not be responsible for any of the Purchasing Entity's costs incurred in cooperating with the audit.

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. Consistent with terms set forth above, 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 resulting in loss or damage to Participating Entity's Data, the Contractor agrees to restore or assist in restoring Data to the Cloud Service with the system to operational capacity from Participating Entity's last available backup copy in compatible format.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall provide the API during the term of the Services. Upon termination of the Services use the API shall cease. Subject to the definitions applicable to "Product(s)" herein as excluded from the definition of Intellectual Property, for purposes of clarity of ownership of any such intellectual property rights shall not include any copyrights, patents, moral rights, trademarks, trade dress, trade secrets, or any other intellectual property rights created outside of or modified or enhanced as a result of the Services or SOW/SD/SLA/PO, including but not limited to any such rights that preexist. If Ancillary Software is licensed to the Purchasing Entity under separate third party license terms, then the Purchasing Entity's use of such software is subject solely to such separate terms.

30. Data Privacy: The Purchasing Entity is responsible for its use of Contractor and non-Contractor products and services, including IRS Pub 1075 as applicable to the Services containing Federal Tax Information and tax data. Prior to entering into an SLA/SOW/SD 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 Parties/Contractor/Purchasing Entity must document the Data Categorization in the Ordering Document / SLA/SOW/SD or Statement of Work. If there is a violation of law or if

there is a breach of security or breach of obligations by a Purchasing Entity applicable to the Cloud Services, IBM may suspend, revoke, or limit the use of the Cloud Service and in which case of a suspension, charges continue to accrue for the Cloud Service for the duration of any such suspension. If the cause of the suspension is reasonably capable of being remedied, IBM will provide notice of what actions must be taken to reinstate the Cloud Service where failure to take such actions within a reasonable time may result in termination of the Cloud Service.

31. Warranties, Disclaimers, and Exclusive Remedies:

a. IBM warrants, as of the effective date of an applicable Ordering Document, it (i) has the necessary experience and expertise to provide the Cloud Service; (ii) has all approvals required by law to comply with its obligations under the Agreement where IBM provides the Cloud Service; (iii) has all rights in the Cloud Service necessary to provide the Cloud Services as described in the relevant Ordering Document; and (iv) it will perform Cloud Services in all material respects as described in its Service Specifications, and Professional Services in a professional manner in accordance with its Service Specifications.

b. Purchasing Entity and IBM each warrants and represents that: (i) it has the authority to enter into the Agreement or Ordering Document; (ii) the persons entering into the Agreement or Ordering Document on its behalf have been duly authorized to do so; and (iii) the Agreement and Ordering Document and the obligations created under them are binding upon it and enforceable against it in accordance with their terms, and do not and will not violate the terms of any other agreement, or any judgment or court order, to which it is bound.

c. If the Services provided to Purchasing Entity were not performed as warranted, Purchasing Entity must promptly provide written notice to IBM that describes the deficiency in the Services (including as applicable, the service request number notifying IBM of the deficiency in the Services).

d. IBM DOES NOT GUARANTEE THAT (i) THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED OR THAT IBM WILL CORRECT ALL SERVICES ERRORS, (ii) THE SERVICES WILL OPERATE IN COMBINATION WITH PURCHASING ENTITY'S CONTENT OR ITS APPLICATIONS, OR WITH ANY OTHER HARDWARE OR SOFTWARE SYSTEMS, SERVICES, OR DATA NOT PROVIDED BY IBM, AND (iii) THE SERVICES WILL MEET PURCHASING ENTITY'S REQUIREMENTS, SPECIFICATIONS, OR EXPECTATIONS. PURCHASING ENTITY ACKNOWLEDGES THAT IBM DOES NOT CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, AND THAT THE SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. IBM IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. IBM IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION, OR SECURITY OF THE SERVICES THAT ARISE FROM PURCHASING ENTITY'S CONTENT, ITS APPLICATIONS, OR THIRD-PARTY CONTENT. IBM WARRANTIES WILL NOT APPLY IF THERE HAS BEEN MISUSE, MODIFICATION, DAMAGE NOT CAUSED BY IBM, FAILURE TO COMPLY WITH INSTRUCTIONS PROVIDED BY IBM, OR IF OTHERWISE STATED IN AN ATTACHMENT OR TD. NON-

IBM SERVICES ARE SOLD UNDER THE AGREEMENT AS-IS, WITHOUT WARRANTIES OF ANY KIND. THIRD PARTIES MAY PROVIDE THEIR OWN WARRANTIES.

e. FOR ANY BREACH OF SERVICES WARRANTY, PURCHASING ENTITY'S EXCLUSIVE REMEDY AND IBM'S ENTIRE LIABILITY SHALL BE THE CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR, IF IBM CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER, PURCHASING ENTITY MAY END THE DEFICIENT SERVICES AND IBM WILL REFUND TO PURCHASING ENTITY THE FEES PAID FOR THE DEFICIENT SERVICES FOR THE PERIOD OF TIME DURING WHICH THE SERVICES WERE DEFICIENT.

f. TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS INCLUDING FOR SOFTWARE, HARDWARE, SYSTEMS, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE.

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 to between a Purchasing Entity and Contractor in a Statement of Work. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support shall be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable. Unless otherwise specified in a Statement of Work or SLA, Purchasing Entity shall have no expectation of access past the termination of the service nor Contractor maintaining Purchasing Entity's Data. Such Transition Plan shall be agreed upon before the end of the service.

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

33. Waiver of Breach: Failure of the Lead State, Master Agreement Administrator, Participating Entity, Purchasing Entity or Contractor 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, Purchasing Entity, or Contractor must be in writing. Waiver by the Lead State Master Agreement Administrator, Participating State Participating Entity or Contractor of any default, right or remedy under this Master Agreement or Participating Addendum, 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 Ordering Document.

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, 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: Provided all Services have been purchased through an IBM Ordering Document, all maintenance or other agreements for services entered into during the duration of an Ordering Document /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. All Services which require payment must be paid in accordance with the invoice even after the expiration of the Master Agreement. 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. IBM reserves the right to negotiate such terms and to decline such Orders.

41. Government Support: Unless otherwise provided in an Ordering Document, 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; (5) Purchasing Entity and Contractor Purchase Order identifier/number(s); (6) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (7) Purchase Order date; and (8) 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. Reserved – IBM does not permit personal use of this master agreement by Public Entity employees.

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 Ordering Document. 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. Reserved

44. Additional Terms and Conditions

a. Restrictions:

The Purchasing Entity may not and may not cause or permit others to:

I. remove or modify any program markings or any notice of IBM's or its licensors' proprietary rights;

II. make the programs or materials resulting from the Services (excluding Purchasing Entity Content and Purchasing Entity Applications) available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific Services the Purchasing Entity has acquired);

III. modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, distribute, republish or download any part of the Services (the foregoing prohibitions include but are not limited to review of data structures or similar materials produced by programs), or access or use the Services in order to build or support, and/or assist a third party in building or supporting, products or Services competitive to IBM;

IV. perform or disclose any benchmark or performance tests of the Services, including the IBM Programs;

V. perform or disclose any of the following security testing of the Services Environment or associated infrastructure: network discovery, port and service identification, vulnerability scanning, password cracking, remote access testing, or penetration testing; and

VI. license, sell, rent, lease, transfer, assign, distribute, host, outsource, permit timesharing or service bureau use, or otherwise commercially exploit or make available the Services, IBM Programs, Ancillary Software, Services Environments or IBM materials, to any third party, other than as expressly permitted under the terms of the applicable Order.

b. Service Specifications:

I. The Services are subject to and governed by Service Specifications applicable to the Purchasing Entity's Order. Service Specifications may define provisioning and management processes applicable to the Services (such as capacity planning), types and quantities of system resources (such as storage allotments), functional and technical aspects of the IBM Programs, as well as any Services deliverables. The Purchasing Entity acknowledges that use of the Services in a manner not consistent with the Service Specifications may adversely affect Services performance and/or may result in additional fees. If the Services permit the Purchasing Entity to exceed the ordered quantity (e.g., soft limits on counts for Users, sessions, storage, etc.), then the Purchasing Entity is responsible for promptly purchasing such additional quantity to account for the Purchasing Entity's excess usage.

II. IBM may make changes or updates to the Services (such as infrastructure, security, technical configurations, application features, etc.) during the Services Period, including to reflect changes in technology, industry practices, patterns of system use, and availability of Third Party Content. The Service Specifications are subject to change at IBM's discretion. Changes or updates will take effect (a) upon a new Order, (b), for Orders previously entered, upon the change effective date for ongoing Services, or (c) upon the renewal date for Services that automatically renew per Ordering Document. The intent of any modification will be to: i) improve or clarify

existing commitments; ii) maintain alignment to current adopted standards and applicable laws; or iii) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of a Cloud Service.

c. Use of the Services:

I. The Purchasing Entity is responsible for identifying and authenticating all Users, for approving access by such Users to the Services, for controlling against unauthorized access by Users, and for maintaining the confidentiality of usernames, passwords and account information. By federating or otherwise associating the Purchasing Entity's and the Purchasing Entity's Users' usernames, passwords and accounts with IBM, the Purchasing Entity accept responsibility for the confidentiality and timely and proper termination of user records in the Purchasing Entity's local (intranet) identity infrastructure or on the Purchasing Entity's local computers. IBM is not responsible for any harm caused by the Purchasing Entity's Users, including individuals who were not authorized to have access to the Services but who were able to gain access because usernames, passwords or accounts were not terminated on a timely basis in the Purchasing Entity's local identity management infrastructure or the Purchasing Entity's local computers. The Purchasing Entity is responsible for all activities that occur under the Purchasing Entity's and the Purchasing Entity's Users' usernames, passwords or accounts or as a result of the Purchasing Entity's or the Purchasing Entity's Users' access to the Services, and agree to notify IBM immediately of any unauthorized use. The Purchasing Entity agrees to make every reasonable effort to prevent unauthorized third parties from accessing the Services.

II. The Purchasing Entity shall not use or permit use of the Services, including by uploading, emailing, posting, publishing or otherwise transmitting any material, including Purchasing Entity Content, Purchasing Entity Applications Content, for any purpose that may (1) menace or harass any person or cause damage or injury to any person or property, (2) involve the publication of any material that is false, defamatory, harassing or obscene, (3) violate privacy rights or promote bigotry, racism, hatred or harm, (4) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters; (5) constitute an infringement of intellectual property or other proprietary rights, or (6) otherwise violate applicable laws, ordinances or regulations. In addition to any other rights afforded to IBM under this Master Agreement, IBM reserves the right, but has no obligation, to take remedial action if any material violates the restrictions in the foregoing sentence (the "Acceptable Use Policy"), including the removal or disablement of access to such material. IBM shall have no liability to the Purchasing Entity in the event that IBM takes such action. The Purchasing Entity shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness and ownership of all of Purchasing Entity Content, Purchasing Entity Applications. To the extent not prohibited by applicable law, the Purchasing Entity agrees to defend and indemnify IBM against any claim arising out of a violation of the Purchasing Entity's obligations under this section.

III. The Purchasing Entity is required to accept all patches, bug fixes, updates, maintenance and service packs (collectively, "Patches") necessary for the proper function and security of the Services, including for the IBM Programs, as such Patches are generally released by IBM as described in the Service Specifications. IBM is not responsible for performance or security issues encountered with the Cloud Services that result from the Purchasing Entity's failure to accept the application of Patches that are necessary for the proper function and security of the Services. Except for emergency or security related maintenance activities, IBM will coordinate with the Purchasing Entity the scheduling of application of Patches, where possible, based on IBM's next available standard maintenance window.

IV. The Purchasing Entity shall obtain at the Purchasing Entity's sole expense any rights and consents from third parties necessary for Purchasing Entity Content, Purchasing Entity Applications, and Third Party Content, as well as other vendor's products provided by the Purchasing Entity that the Purchasing Entity use with the Services, including such rights and consents as necessary for IBM to perform the Services under this Master Agreement.

V. The Purchasing Entity remains solely responsible for the Purchasing Entity's regulatory compliance in connection with the Purchasing Entity's use of the Services. The Purchasing Entity is responsible for making IBM aware of any technical requirements that result from the Purchasing Entity's regulatory obligations prior to entering into an Order governed by this Master Agreement. IBM will cooperate with the Purchasing Entity's efforts to determine whether use of the standard IBM Services offering is consistent with those requirements. Additional fees may apply to any additional work performed by IBM or changes to the Services.

d. Trial Use and Pilot Cloud Services:

I. For certain Cloud Services, IBM may make available "trials" and "conference room pilots" for non-production evaluation purposes. Cloud trials and conference room pilots must be ordered under a separate agreement.

II. IBM may make available "production pilots" for certain Cloud Services under this Master Agreement. Production pilots ordered by the Purchasing Entity is described in the Service Specifications applicable to the Purchasing Entity's Order, and are provided solely for the Purchasing Entity to evaluate and test Cloud Services for the Purchasing Entity's internal business purposes. The Purchasing Entity may be required to order certain Professional Services as a prerequisite to an Order for a production pilot.

e. Services Period; End of Services:

I. Services provided under this Master Agreement shall be provided for the Services Period defined in the Purchasing Entity's Order, unless earlier suspended or terminated in accordance with this Master Agreement or the Order.

II. IBM may suspend or limit, to the extent necessary, Participating Entity's use of a Service if IBM determines there is a material breach of Purchasing Entity's

obligations, a security breach, violation of law, or breach of the terms as set forth in 7b of the IBM CSA.

III. If the Purchasing Entity has used an IBM Financing Division contract to pay for the fees due under an Order and the Purchasing Entity is in default under that contract, the Purchasing Entity may not use the Services that are subject to such contract.

f. Limitation of Liability:

A. CONTRACTOR'S AGGREGATE LIABILITY FOR ALL DAMAGES ARISING OUT OF OR RELATED TO THIS MASTER AGREEMENT OR A PURCHASING ENTITY'S ORDER, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED THE GREATER OF (i) TWO (2) TIMES THE TOTAL AMOUNTS ACTUALLY PAID TO IBM IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY LESS ANY REFUNDS OR CREDITS RECEIVED BY THE PURCHASING ENTITY FROM CONTRACTOR UNDER SUCH ORDER OR (ii) ONE MILLION DOLLARS (U.S.$1,000,000).

B. NOTWITHSTANDING THE ABOVE, NEITHER THE CONTRACTOR NOR THE PURCHASING ENTITY SHALL BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, PUNITIVE OR SPECIAL DAMAGES OF ANY KIND ARISING DIRECTLY OR INDIRECTLY OUT OF THIS MASTER AGREEMENT OR A PURCHASING ENTITY'S ORDER, INCLUDING, WITHOUT LIMITATION, DAMAGES RESULTING FROM LOSS OF USE OR LOSS OF PROFIT OR REVENUE (EXCLUDING FEES UNDER THIS MASTER AGREEMENT), DATA, OR DATA USE BY THE PURCHASING ENTITY, THE CONTRACTOR, OR BY OTHERS.

C. Contractor's obligation to indemnify for (i) infringement claims or damages under Sections 13(b) or (ii) claim(s) of bodily injury and tangible personal property damage under Section 13(a) shall apply without regard to whether the damages under such claim(s) (y) are classified as direct, indirect, or otherwise, or (z) exceed the limits on liability under this Section 44(f) (Additional Terms and Conditions: Limitation of Liability).

g. Third Party Web Sites, Content, Products and Services:

I. The Services may enable the Purchasing Entity to link to, transmit Purchasing Entity Content to, or otherwise access, other Web sites, platforms, content, products, services, and information of third parties. IBM does not control and is not responsible for such Web sites or platforms or any such content, products, services and information accessible from or provided through the Services, and the Purchasing Entity bear all risks associated with access to and use of such Web sites and third party content, products, services and information.

II. Any Third Party Content made accessible by IBM is provided on an "as-is" and "as available" basis without any warranty of any kind. Third Party Content may be indecent, offensive, inaccurate, infringing or otherwise objectionable or unlawful, and

the Purchasing Entity acknowledge that IBM is not responsible for and under no obligation to control, monitor or correct Third Party Content; however, IBM reserves the right to take remedial action if any such content violates applicable restrictions under this Master Agreement, including the removal of, or disablement of access to, such content. IBM disclaims all liabilities arising from or related to Third Party Content.

III. The Purchasing Entity acknowledge that: (1) the nature, type, quality and availability of Third Party Content may change at any time during the Services Period, and (2) features of the Services that interoperate with third parties (each, a "Third Party Service"), depend on the continuing availability of such third parties' respective application programming interfaces (APIs) for use with the Services. IBM may update, change or modify the Services under this Master Agreement as a result of a change in, or unavailability of, such Third Party Content, Third Party Services or APIs. If any third party ceases to make its Third Party Content or APIs available on reasonable terms for the Services, as determined by IBM in its sole discretion, IBM may cease providing access to the affected Third Party Content or Third Party Services without any liability to the Purchasing Entity. Any changes to Third Party Content, Third Party Services or APIs, including their availability or unavailability, during the Services Period does not affect the Purchasing Entity's obligations under this Master Agreement or the applicable Order, and the Purchasing Entity will not be entitled to any refund, credit or other compensation due to any such changes.

IV. Any Third Party Content that the Purchasing Entity store in the Purchasing Entity's Services Environment will count towards any storage or other allotments applicable to the Cloud Services that the Purchasing Entity ordered.

h. Service Analyses:

IBM may (i) compile statistical and other information related to the performance, operation and use of the Services, and (ii) use data from the Services Environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as "Service Analyses"). IBM may make Service Analyses publicly available; however, Service Analyses will not incorporate Purchasing Entity Content or Confidential Information in a form that could serve to identify the Purchasing Entity or any individual, and Service Analyses do not constitute Personal Data. IBM retains all intellectual property rights in Service Analyses.

i. Export:

a. Export laws and regulations of the United States and any other relevant local export laws and regulations apply to the Services. the Purchasing Entity agree that such export laws govern the Purchasing Entity's use of the Services (including technical data) and any Services deliverables provided under this Master Agreement, and the Purchasing Entity agree to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). the Purchasing Entity agree that no data, information, software programs and/or materials resulting from Services (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws

b. The Purchasing Entity acknowledge that the Cloud Services are designed with capabilities for the Purchasing Entity and the Purchasing Entity's Users to access the Services Environment without regard to geographic location and to transfer or otherwise move Purchasing Entity Content and Purchasing Entity Applications between the Services Environment and other locations such as User workstations. The Purchasing Entity is solely responsible for the authorization and management of User accounts, as well as export control and geographic transfer of Purchasing Entity Content and Purchasing Entity Applications.

j. Notice:

i. All notices under this Master Agreement must be in writing and sent to the business address specified for this Master Agreement, unless a party designates in writing a different address.

ii. IBM may give notices applicable to IBM's Cloud Services customer base by means of a general notice on the IBM portal for the Cloud Services, and notices specific to the Purchasing Entity by electronic mail to the Purchasing Entity's e-mail address on record in IBM's account information or by written communication sent by first class mail or pre-paid post to the Purchasing Entity's address on record in IBM's account information.

k. Miscellaneous:

i. If any term of this Master Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective and such term shall be replaced with another term consistent with the purpose and intent of this Master Agreement.

ii. The purchase of Cloud Services, Professional Services, or other service offerings, programs or products are all separate offers and separate from any other Order. The Purchasing Entity understands that the Purchasing Entity may purchase Cloud Services, Professional Services, or other service offerings, programs or products independently of any other Order. The Purchasing Entity's obligation to pay under any Order is not contingent on performance of any other service offerings or delivery of programs or products.

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 and Exhibits contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum or otherwise with a Participating or Purchasing Entity as set forth herein. For purposes of clarity, each Service Description, SOW, Order, or Transaction Document may contain references to associated documents or terms which, upon acceptance, will be incorporated as part of the Cloud Services as allowed under this Master Agreement. 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, unless ~~even if~~ use of such Services requires an affirmative "acceptance" of those Additional Terms before

access is permitted. If any provision of the Master Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect and nothing in this Agreement affects the statutory rights of consumers that cannot be waived or limited by contract.

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, Transaction Document (TD) and/or other contract documents (including compliance with applicable laws), or (4) at the Purchasing Entity's written request.

Unless set forth in an applicable TD, 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 or is publicly available. 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 so that 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 Data 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 security measures described in an applicable TD.

b. All Non-Public Data obtained from the Purchasing Entity 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 if, and to the extent as set forth in, an applicable TD regarding security requirements of data classification. If and unless otherwise stipulated in an applicable TD, the Contractor may not be responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the applicable TD, or otherwise made a part of the Master Agreement.

d. If stipulated in the applicable TD the Contractor shall encrypt all Non-Public Data at rest and in transit based upon the applicable security requirements set forth and agreed to in the applicable TD. 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 applicable TD.

e. At no time shall any Data or processes defined as Confidential — 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 Purchasing Entity Data in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

g. Nothing contained herein shall be deemed to enlarge or otherwise change the Contractor's responsibilities for treatment of Confidential Information as set forth in Section 8 of the Master Agreement.

3. Data Location: As selected by Purchasing Entity from available Contractor data centers, the Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S and 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 and general administrative 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. Data Breach Notification: The Contractor shall inform the Purchasing Entity of Data Breach related to Purchasing Entity's Data within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or applicable TD. Such notice will be based upon Purchasing Entity's selection of security requirements described in applicable TD.

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

b. Security Breach Reporting Requirements: Unless otherwise stipulated in a signed writing, the Contractor shall report a Security Breach subject to the same requirements in section 4(c) below related to its service under the Master Agreement, Participating Addendum, or applicable TD to the appropriate Purchasing Entity.

c. Data Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed Data Breach that affects the security of any Purchasing Entity data that is subject to applicable Data Breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity as stipulated within the applicable TD (but no later than 72 hours after Contractor determines that Purchasing Entity Personal Data has been subject to a Data Breach), unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

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

a. The Contractor, shall notify the appropriate Purchasing Entity in accordance with the agreed upon notification requirements in the applicable TD.

b. The Contractor shall notify the appropriate Purchasing Entity identified contact as described in TD, unless shorter time is required by applicable law. If the Contractor confirms that there is a Data Breach, the Contractor shall (1) cooperate with the Purchasing Entity as stipulated in the applicable TD to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) maintain & follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notifications terms of the Contractor's Cloud Services Agreement.

c. Unless otherwise stipulated, if a Purchasing Entity retained Contractor to encrypt Personal Data in accordance with an applicable TD, and a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall, subject to the conditions set forth in subsections (A) and (B) of this section, bear the costs (which shall be deemed direct damages) 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) completion of all corrective actions related to the delivery of the Service as reasonably determined by Contractor based on root cause analysis and findings, provided however that:

(A) CONTRACTOR'S ENTIRE OBLIGATION FOR ALL DAMAGES AND EXPENSES RELATED TO A DATA BREACH SHALL BE SUBJECT TO THE LIMITATION SET FORTH IN SECTION 44.f. OF THE MASTER AGREEMENT TERMS AND CONDITIONS, WHICH SHALL BE MODIFIED AS FOLLOWS SOLELY IN THE EVENT OF A DATA BREACH: (i) IN CONNECTION WITH ORDERS RECEIVED IN AGGREGATE VALUE BETWEEN ONE MILLION DOLLARS (U.S. $1,000,000) AND FIVE MILLION DOLLARS (U.S. $5,000,000), SUBSECTION 44.f.A.(ii) SHALL BE MODIFIED TO READ "TWO MILLION, FIVE HUNDRED THOUSAND DOLLARS (U.S. $2,500,000)"; AND (ii) IN CONNECTION WITH ORDERS RECEIVED IN AGGREGATE VALUE THAT EXCEEDS FIVE MILLION DOLLARS (U.S. $5,000,000), SUBSECTION 44.f.A.(ii) SHALL BE MODIFIED TO READ "THREE MILLION DOLLARS (U.S. $3,000,000)"; and

(B) this Section 5.c sets forth Contractor's entire obligation and, when applicable, shall constitute Purchasing Entity's sole and exclusive remedy for all damages and expenses related to a Data Breach.

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 Purchasing Entity's Data. The Contractor shall not respond to subpoenas or service of process related to the Purchasing Entity without first notifying the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

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

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 except for material breach including non-payment, security breach or violation of law by Purchasing Entity.

c. In the event of early termination of any Services or agreement in entirety except for material breach including, as applicable, non-payment, security breach or violation of law, the Contractor shall not take any action to intentionally erase any Purchasing Entity's Data for a period to be outlined in the applicable TD. After such day period outline in the applicable TD, the Contractor shall have no obligation to maintain or provide any Purchasing Entity Data and shall thereafter, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. Any charges or fees assessed by Contractor for access and retrieval of Purchasing Entity Data, if any, shall be at Contractor's standard charges and fees for such access and retrieval.

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 applicable TD.

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, if stipulated in an applicable TD by the Purchasing Entity. Such Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods.

8. Background Checks:

a. Contractor follows a mandated set of employment verification requirements for all new hires, including regular, fixed term, supplementals, part time, interns, early professional and

professional hires. These standards apply to Contractor's wholly owned subsidiaries and joint ventures. The requirements currently include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each country is responsible for implementing the above requirements in their hiring process as applicable and permissible pursuant to each country's local laws.

When requested under an applicable TD, the Contractor shall conduct a background investigation in accordance with Contractor's internal process. This investigation may be at the Purchasing Entity's expense. Contractor will conduct the background and/or verification checks in accordance with Contractor's polices and applicable law and background report may include a check of a national criminal database as well as the OFAC Listing.

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

c. If any of the stated personnel providing services under an applicable TD is not acceptable to the Purchasing Entity as a result of the background investigation, the Purchasing Entity, shall have the option to either (1) request replacement of the person, or (2) terminate the Participating Addendum and any related service agreement in accordance with the Termination Section of the Master Agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports specified in an applicable TD to the Purchasing Entity Depending upon offering being purchased, reports may include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or applicable TD.

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

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit financial data and records for conformance with Section 26 of the Master Agreement, Records and Audit Administration.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and upon request to a Purchasing Entity with a written non-disclosure agreement. A redacted Service Organization Control (SOC) 2 audit report or equivalent third-party audit will be provided. Data Center audit reports are Confidential Information of Contractor and shall be treated as

such at all times. Access to such reports under an Open Records or Freedom of Information Act provision shall be addressed as needed in the Participating Addendum under which a Purchasing Entity procures a Cloud Service. Physical access to data centers is prohibited except as required by law.

12. Change Control and Advance Notice: The Contractor shall give reasonable notice as defined in an applicable TD to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that Contractor expects 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 may include 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 at no cost. Additional costs may be required for specific customer requests, and these updates and upgrades will be based on list price less applicable contract discounts.

13. Security: Based upon selection of SaaS Service and 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 as described in an applicable TD.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements in accordance with Master Agreement paragraph 8 Confidentiality, Non-Disclosure, and Injunctive Relief, and limit staff knowledge of Purchasing Entity data to that which is 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 subject to compliance with Master Agreement Section 17 Laws. Contractor shall specify in an applicable TD 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 shared responsibilities of the parties described in an applicable TD. The system shall be available as described in the applicable TD (with agreed-upon maintenance downtime) and provide service to customers as defined in the applicable TD.

17. Subcontractor Disclosure: Contractor shall identify corporate entities related to services provided under this Master Agreement, who shall be involved in any application development and/or operations. For purposes of clarity, Contractor is not required to identify its employees who are providing Services.

18. Reserved.

19. Business Continuity and Disaster Recovery: If requested as part of the Services, the Contractor shall provide a business continuity and disaster recovery (BC/DR) plan upon request, based on the Purchasing Entity's recovery time objective (RTO) of XXX hours/days (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) As part of the BC/DR services, Contractor will 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 legal requirements applicable including Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or other legally applicable state laws or administrative regulations identified by the Participating Entity as set forth in an applicable TD.

21. Web Services: The Contractor shall use Web services or other services as described in an applicable TD to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: When a Statement of Work require Contractor to provide 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 Protected Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Protected Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: If set forth in an applicable TD, Contractor grants to a Purchasing Entity the ability 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. Except as set forth in the Master Agreement, no Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement or in an applicable TD.

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

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

Unless set forth in a TD, 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 or is publicly available. 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 so that 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 Data 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 security measures described in an applicable TD.

b. All Non-Public Data obtained from the Purchasing Entity 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 if, and to the extent as set forth in, an applicable TD regarding security requirements of data classification. If and unless otherwise stipulated in an applicable TD, the Contractor may not be responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the applicable TD, or otherwise made a part of the Master Agreement.

d. If stipulated in the applicable TD, the Contractor shall encrypt all Non-Public Data at rest and in transit based upon the applicable security requirements set forth and agreed to in the applicable TD. 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 applicable TD.

e. At no time shall any Data or processes defined as Confidential — 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 Purchasing Entity Data in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

g. Nothing contained herein shall be deemed to enlarge or otherwise change the Contractor's responsibilities for treatment of Confidential Information as set forth in Section 8 of the Master Agreement.

3. Data Location: As selected by Purchasing Entity from available Contractor data centers, the Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S and 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 and general administrative 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. Data Breach Notification: The Contractor shall inform the Purchasing Entity of Data Breach related to Purchasing Entity's Data within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or applicable TD. Such notice will be based upon Purchasing Entity's selection of security requirements described in applicable TD.

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

b. Security Breach Reporting Requirements: Unless otherwise stipulated in a signed writing, the Contractor shall report a Security Breach subject to the same requirements in section 4(c) below related to its service under the Master Agreement, Participating Addendum, or applicable TD to the appropriate Purchasing Entity.

c. Data Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed Data Breach that affects the security of any Purchasing Entity data that is subject to applicable Data Breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity as stipulated within the applicable TD (but no later than 72 hours after Contractor determines that Purchasing Entity Personal Data has been subject to a Data Breach), unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

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

a. The Contractor, shall notify the appropriate Purchasing Entity in accordance with the agreed upon notification requirements in the applicable TD.

b. The Contractor shall notify the appropriate Purchasing Entity identified contact as described in TD, unless shorter time is required by applicable law. If the Contractor confirms that there is a Data Breach, the Contractor shall (1) cooperate with the Purchasing Entity as stipulated in the applicable TD to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) maintain & follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notifications terms of the Contractor's Cloud Services Agreement.

c. Unless otherwise stipulated, if a Purchasing Entity retained Contractor to encrypt Personal Data in accordance with an applicable TD, and a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall, subject to the conditions set forth in subsections (A) and (B) of this section, bear the costs (which shall be deemed direct damages) 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) completion of all corrective actions related to the delivery of the Service as reasonably determined by Contractor based on root cause analysis and findings, provided however that:

(A) CONTRACTOR'S ENTIRE OBLIGATION FOR ALL DAMAGES AND EXPENSES RELATED TO A DATA BREACH SHALL BE SUBJECT TO THE LIMITATION SET FORTH IN SECTION 44.f. OF THE MASTER AGREEMENT TERMS AND CONDITIONS, WHICH SHALL BE MODIFIED AS FOLLOWS SOLELY IN THE EVENT OF A DATA BREACH: (i) IN CONNECTION WITH ORDERS RECEIVED IN AGGREGATE VALUE BETWEEN ONE MILLION DOLLARS (U.S. $1,000,000) AND FIVE MILLION DOLLARS (U.S. $5,000,000), SUBSECTION 44.f.A.(ii) SHALL BE MODIFIED TO READ "TWO MILLION, FIVE HUNDRED THOUSAND DOLLARS (U.S. $2,500,000)"; AND (ii) IN CONNECTION WITH ORDERS RECEIVED IN AGGREGATE VALUE THAT EXCEEDS FIVE MILLION DOLLARS (U.S. $5,000,000), SUBSECTION 44.f.A.(ii) SHALL BE MODIFIED TO READ "THREE MILLION DOLLARS (U.S. $3,000,000)"; and

(B) this Section 5.c sets forth Contractor's entire obligation and, when applicable, shall constitute Purchasing Entity's sole and exclusive remedy for all damages and expenses related to a Data Breach.

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 Purchasing Entity's Data. The Contractor shall not respond to subpoenas or service of process related to the Purchasing Entity without first notifying the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

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

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 except for material breach including non-payment, security breach or violation of law by Purchasing Entity.

c. In the event of early termination of any Services or agreement in entirety except for material breach including, as applicable, non-payment, security breach or violation of law, the Contractor shall not take any action to intentionally erase any Purchasing Entity's Data for a period to be outlined in the applicable TD. After such day period outline in the applicable TD, the Contractor shall have no obligation to maintain or provide any Purchasing Entity Data and shall thereafter, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. Any charges or fees assessed by Contractor for access and retrieval of Purchasing Entity Data, if any, shall be at Contractor's standard charges and fees for such access and retrieval.

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 applicable TD.

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, if stipulated in an applicable TD by the Purchasing Entity. Such Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods.

8. Background Checks:

a. Contractor follows a mandated set of employment verification requirements for all new hires, including regular, fixed term, supplementals, part time, interns, early professional and

professional hires. These standards apply to Contractor's wholly owned subsidiaries and joint ventures. The requirements currently include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each country is responsible for implementing the above requirements in their hiring process as applicable and permissible pursuant to each country's local laws.

When requested under an applicable TD, the Contractor shall conduct a background investigation in accordance with Contractor's internal process. This investigation may be at the Purchasing Entity's expense. Contractor will conduct the background and/or verification checks in accordance with Contractor's polices and applicable law and background report may include a check of a national criminal database as well as the OFAC Listing.

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

c. If any of the stated personnel providing services under an applicable TD is not acceptable to the Purchasing Entity as a result of the background investigation, the Purchasing Entity, shall have the option to either (1) request replacement of the person, or (2) terminate the Participating Addendum and any related service agreement in accordance with the Termination Section of the Master Agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports specified in an applicable TD to the Purchasing Entity Depending upon offering being purchased, reports may include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or applicable TD.

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

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit financial data and records for conformance with Section 26 of the Master Agreement, Records and Audit Administration.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and upon request to a Purchasing Entity with a written non-disclosure agreement. A redacted Service Organization Control (SOC) 2 audit report or equivalent third-party audit will be provided. Data Center audit reports are Confidential Information of Contractor and shall be treated as

such at all times. Access to such reports under an Open Records or Freedom of Information Act provision shall be addressed as needed in the Participating Addendum under which a Purchasing Entity procures a Cloud Service. Physical access to data centers is prohibited except as required by law.

12. Change Control and Advance Notice: The Contractor shall give reasonable notice as defined in an applicable TD to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that Contractor expects 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 may include 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 at no cost. Additional costs may be required for specific customer requests, and these updates and upgrades will be based on list price less applicable contract discounts.

13. Security: Based upon selection of PaaS Service and 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 as described in an applicable TD.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements in accordance with Master Agreement paragraph 8 Confidentiality, Non-Disclosure, and Injunctive Relief, and limit staff knowledge of Purchasing Entity data to that which is 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 subject to compliance with Master Agreement Section 17 Laws. Contractor shall specify in an applicable TD 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 shared responsibilities of the parties described in an applicable TD. The system shall be available as described in the applicable TD (with agreed-upon maintenance downtime) and provide service to customers as defined in the applicable TD

17. Subcontractor Disclosure: Contractor shall identify corporate entities related to services provided under this Master Agreement, who shall be involved in any application development and/or operations. For purposes of clarity, Contractor is not required to identify its employees who are providing Services.

18. Business Continuity and Disaster Recovery: If requested as part of the Services, the Contractor shall provide a business continuity and disaster recovery (BC/DR) plan upon request, based on the Purchasing Entity's recovery time objective (RTO) of XXX hours/days (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) As part of the BC/DR services, Contractor will work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to legal requirements applicable including Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or other legally applicable state laws or administrative regulations identified by the Participating Entity as set forth in an applicable TD.

20. Web Services: The Contractor shall use Web services or other services as described in an applicable TD to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: When a Statement of Work require Contractor to provide 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 Protected Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Protected Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: If set forth in an applicable TD, Contractor grants to a Purchasing Entity the ability to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation. Except as set forth in the Master Agreement, no Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement or in an applicable TD.

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

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

Unless set forth in a TD, 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 or is publicly available. 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 so that 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 Data 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 security measures described in applicable TD.

b. All Non-Public Data obtained from the Purchasing Entity 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 if, and to the extent as set forth in, an applicable TD regarding security requirements of data classification. If and unless otherwise stipulated in an applicable TD, the Contractor may not be responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the applicable TD, or otherwise made a part of the Master Agreement.

d. If stipulated in the applicable TD, the Contractor shall encrypt all Non-Public Data at rest and in transit based upon the applicable security requirements set forth and agreed to in the applicable TD. 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 applicable TD.

e. At no time shall any Data or processes defined as Confidential — 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 Purchasing Entity Data in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

g. Nothing contained herein shall be deemed to enlarge or otherwise change the Contractor's responsibilities for treatment of Confidential Information as set forth in Section 8 of the Master Agreement.

3. Data Location: As selected by Purchasing Entity from available Contractor data centers, the Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S and 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 and general administrative 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. Data Breach Notification: The Contractor shall inform the Purchasing Entity of Data Breach related to Purchasing Entity's Data within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or applicable TD. Such notice will be based upon Purchasing Entity's selection of security requirements described in the applicable TD.

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

b. Security Breach Reporting Requirements: Unless otherwise stipulated in a signed writing, the Contractor shall report a Security Breach subject to the same requirements in section 4(c) below related to its service under the Master Agreement, Participating Addendum, or applicable TD to the appropriate Purchasing Entity.

c. Data Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed Data Breach that affects the security of any Purchasing Entity data that is subject to applicable Data Breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity as stipulated within the applicable TD (but no later than 72 hours after Contractor determines that Purchasing Entity Personal Data has been subject to a Data Breach), unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

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

a. The Contractor, shall notify the appropriate Purchasing Entity in accordance with the agreed upon notification requirements in the applicable TD.

b. The Contractor shall notify the appropriate Purchasing Entity identified contact as described in TD, unless shorter time is required by applicable law. If the Contractor confirms that there is a Data Breach, the Contractor shall (1) cooperate with the Purchasing Entity as stipulated in the applicable TD to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) maintain & follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notifications terms of the Contractor's Cloud Services Agreement.

c. Unless otherwise stipulated, if a Purchasing Entity retained Contractor to encrypt Personal Data in accordance with an applicable TD, and a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall, subject to the conditions set forth in subsections (A) and (B) of this section, bear the costs (which shall be deemed direct damages) 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) completion of all corrective actions related to the delivery of the Service as reasonably determined by Contractor based on root cause analysis and findings, provided however that:

(A) CONTRACTOR'S ENTIRE OBLIGATION FOR ALL DAMAGES AND EXPENSES RELATED TO A DATA BREACH SHALL BE SUBJECT TO THE LIMITATION SET FORTH IN SECTION 44.f. OF THE MASTER AGREEMENT TERMS AND CONDITIONS, WHICH SHALL BE MODIFIED AS FOLLOWS SOLELY IN THE EVENT OF A DATA BREACH: (i) IN CONNECTION WITH ORDERS RECEIVED IN AGGREGATE VALUE BETWEEN ONE MILLION DOLLARS (U.S. $1,000,000) AND FIVE MILLION DOLLARS (U.S. $5,000,000), SUBSECTION 44.f.A.(ii) SHALL BE MODIFIED TO READ "TWO MILLION, FIVE HUNDRED THOUSAND DOLLARS (U.S. $2,500,000)"; AND (ii) IN CONNECTION WITH ORDERS RECEIVED IN AGGREGATE VALUE THAT EXCEEDS FIVE MILLION DOLLARS (U.S. $5,000,000), SUBSECTION 44.f.A.(ii) SHALL BE MODIFIED TO READ "THREE MILLION DOLLARS (U.S. $3,000,000)"; and

(B) this Section 5.c sets forth Contractor's entire obligation and, when applicable, shall constitute Purchasing Entity's sole and exclusive remedy for all damages and expenses related to a Data Breach.

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 Purchasing Entity's Data. The Contractor shall not respond to subpoenas or service of process related to the Purchasing Entity without first notifying the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

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

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 except for material breach including non-payment, security breach or violation of law by Purchasing Entity.

c. In the event of early termination of any Services or agreement in entirety except for material breach including, as applicable, non-payment, security breach or violation of law, the Contractor shall not take any action to intentionally erase any Purchasing Entity's Data for a period to be outlined in the applicable TD. After such day period outline in the applicable TD, the Contractor shall have no obligation to maintain or provide any Purchasing Entity Data and shall thereafter, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. Any charges or fees assessed by Contractor for access and retrieval of Purchasing Entity Data, if any, shall be at Contractor's standard charges and fees for such access and retrieval.

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 applicable TD.

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, if stipulated in an applicable TD by the Purchasing Entity. Such Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods.

8. Background Checks:

a. Contractor follows a mandated set of employment verification requirements for all new hires, including regular, fixed term, supplementals, part time, interns, early professional and

professional hires. These standards apply to Contractor's wholly owned subsidiaries and joint ventures. The requirements currently include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each country is responsible for implementing the above requirements in their hiring process as applicable and permissible pursuant to each country's local laws.

When requested under an applicable TD, the Contractor shall conduct a background investigation in accordance with Contractor's internal process. This investigation may be at the Purchasing Entity's expense. Contractor will conduct the background and/or verification checks in accordance with Contractor's polices and applicable law and background report may include a check of a national criminal database as well as the OFAC Listing.

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

c. If any of the stated personnel providing services under an applicable TD is not acceptable to the Purchasing Entity as a result of the background investigation, the Purchasing Entity, shall have the option to either (1) request replacement of the person, or (2) terminate the Participating Addendum and any related service agreement in accordance with the Termination Section of the Master Agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports specified in an applicable TD to the Purchasing Entity Depending upon offering being purchased, reports may include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or applicable TD.

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

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit financial data and records for conformance with Section 26 of the Master Agreement, Records and Audit Administration.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and upon request to a Purchasing Entity with a written non-disclosure agreement. A redacted Service Organization Control (SOC) 2 audit report or equivalent third-party audit will be provided. Data Center audit reports are Confidential Information of Contractor and shall be treated as

such at all times. Access to such reports under an Open Records or Freedom of Information Act provision shall be addressed as needed in the Participating Addendum under which a Purchasing Entity procures a Cloud Service. Physical access to data centers is prohibited except as required by law.

12. Change Control and Advance Notice: The Contractor shall give reasonable notice as defined in an applicable TD to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that Contractor expects 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 may include 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 at no cost. Additional costs may be required for specific customer requests, and these updates and upgrades will be based on list price less applicable contract discounts.

13. Security: Based upon selection of IaaS Service and 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 as described in an applicable TD.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements in accordance with Master Agreement paragraph 8 Confidentiality, Non-Disclosure, and Injunctive Relief, and limit staff knowledge of Purchasing Entity data to that which is 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 subject to compliance with Master Agreement Section 17 Laws. Contractor shall specify in an applicable TD 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 shared responsibilities of the parties described in an applicable TD. The system shall be available as described in the applicable TD (with agreed-upon maintenance downtime) and provide service to customers as defined in the applicable TD.

17. Subcontractor Disclosure: Contractor shall identify corporate entities related to services provided under this Master Agreement, who shall be involved in any application development and/or operations. For purposes of clarity, Contractor is not required to identify its employees who are providing Services.

18. Business Continuity and Disaster Recovery: If requested as part of the Services, the Contractor shall provide a business continuity and disaster recovery (BC/DR) plan upon request, based on the Purchasing Entity's recovery time objective (RTO) of XXX hours/days (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) As part of the BC/DR services, Contractor will work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Subscription Terms: If set forth in an applicable TD, Contractor grants to a Purchasing Entity the ability to: (i) access and use the Service for its business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation. Except as set forth in the Master Agreement, no Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement or in an applicable TD.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

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

1.2 Risk Categorization.*

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

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

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

** In the Hybrid Deployment Model, some of the systems, applications, and database may reside on customer premises outside of IBM Cloud infrastructure. Therefore, those components must support the Data Risk classifications, as specified in the Table above for the end-to-end cloud solution to comply with the requirement in this document.

*** While the Community Cloud is not a standard Deployment Model, as per IBM Cloud terminology, it is supported on IBM Cloud platform.

****While IBM PaaS offerings can support the Data Risk classifications indicated, IBM recommends reviewing each use case individually to confirm its compliance with a given Data Risk classification and the state's security posture.

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: International Business Machines Corp.

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,

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

Cloud Service Model: Infrastructure as a Service (IaaS)	
Description	Minimum Discount % Off
IaaS Minimum Discount % * (applies to all OEM's offered within this IaaS model)	3.00%
Average IaaS OEM Discount Off	**3.00%**

Cloud Service Model: Platform as a Service (PaaS)	
Description	Minimum Discount % Off
PaaS Minimum Discount % * (applies to all OEM's offered within this PaaS model)	3.00%
Average PaaS OEM Discount Off	**3.00%**

Cloud Service Model: Software as a Service (SaaS)	
Description	Minimum Discount % Off
SaaS Minimum Discount % * (applies to all OEM's offered within this SaaS model)	3.00%
Average SaaS OEM Discount Off*	**3.00%**

Additional Value Added Services

	Onsite Hourly Rate		Remote Hourly Rate	
Item Description	**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services	N/A	N/A	N/A	N/A
Professional Services				
Architect I	$ 151.87	$ 153.02		
Architect II	$ 182.75	$ 184.14		
Architect III	$ 213.63	$ 215.25		
Architect IV	$ 258.19	$ 260.14		
Architect V	$ 321.53	$ 323.96		
Business Analyst I	$ 121.50	$ 122.42		
Business Analyst II	$ 167.57	$ 168.83		
Business Analyst III	$ 213.63	$ 215.25		
Business Analyst IV	$ 258.19	$ 260.14		
Business Analyst V	$ 321.53	$ 323.96		
Consultant I	$ 209.23	$ 210.82		
Consultant II	$ 235.91	$ 237.69		
Consultant III	$ 258.19	$ 260.14		
Consultant IV	$ 298.68	$ 300.94		
Consultant V	$ 339.78	$ 342.35		
Database Administrator I	$ 121.50	$ 122.42		
Database Administrator II	$ 136.69	$ 137.72		
Database Administrator III	$ 151.88	$ 153.02		
Database Administrator IV	$ 217.89	$ 219.53		
Database Administrator V	$ 283.14	$ 285.28		
Project Coordinator I	$ 96.19	$ 96.92		
Project Coordinator II	$ 105.57	$ 106.37		
Project Coordinator III	$ 116.43	$ 117.31		
Project Coordinator IV	$ 136.69	$ 137.72		
Project Manager I	$ 117.62	$ 118.51		
Project Manager II	$ 119.98	$ 120.88		
Project Manager III	$ 177.56	$ 178.90		
Project Manager IV	$ 227.81	$ 229.53		
Project Manager V	$ 321.52	$ 323.95		
Software Lab Services I	$ 242.82	$ 244.66		
Software Lab Services II	$ 260.09	$ 262.06		
Software Lab Services III	$ 277.38	$ 279.47		
Software Lab Services IV	$ 303.30	$ 305.59		
Software Lab Services V	$ 339.77	$ 342.34		
Systems Administrator - Client, Enterprise and Data Center Technologies I	$ 122.49	$ 123.42		
Systems Administrator - Client, Enterprise and Data Center Technologies II	$ 136.17	$ 137.20		
Systems Administrator - Client, Enterprise and Data Center Technologies III	$ 149.85	$ 150.98		
Systems Administrator - Client, Enterprise and Data Center Technologies IV	$ 171.11	$ 172.40		
Systems Administrator - Client, Enterprise and Data Center Technologies V	$ 205.30	$ 206.86		
Technical Systems and Solutions Specialist I	$ 121.50	$ 122.42		
Technical Systems and Solutions Specialist II	$ 167.57	$ 168.83		

Attachment C - Pricing Discounts and Schedule

Contractor: International Business Machines Corp.

	Technical Systems and Solutions Specialist III	$ 213.63	$ 215.25
	Technical Systems and Solutions Specialist IV	$ 236.11	$ 237.90
	Technical Systems and Solutions Specialist V	$ 263.95	$ 265.95
	IT Analyst - Solutions I	$ 111.38	$ 112.22
	IT Analyst - Solutions II	$ 124.03	$ 124.97
	IT Analyst - Solutions III	$ 136.69	$ 137.72
	IT Analyst - Solutions IV	$ 151.88	$ 153.02
	IT Analyst - Solutions V	$ 183.52	$ 184.91
Partner Services		N/A	N/A
Training Deployment Services		N/A	N/A

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

IBM PROPOSAL TO:

State of Utah

For Cloud Solutions RFP

Prepared for State of Utah

By Karen Schneider
International Business Machines
3935 Acacia Ave.
Bonita, CA 91902
Telephone 720-397-5563
Email kasch@us.ibm.com

July 6, 2018

Table of Contents

6. Technical Response **1**

Figure List

Figure 1: Resource Pool - Public Cloud - Dedicated Model 3
Figure 2: IBM Cloud UI - – Sample User Notifications 14
Figure 3: Security and Compliance in the Layered IBM Cloud architecture 43
Figure 4: IBM Cloud Security Architecture - Public and IBM Cloud Dedicated Platform 44
Figure 5: IBM Cloud - Outage Types..... 51
Figure 6: IBM Cloud - Customer credits due to SLA meeting failure 51
Figure 7: IBM Cloud - North America Data Centers 60
Figure 8: IBM Cloud Support Offerings 68
Figure 9: IBM Cloud APM - Portfolio Management Report..... 70
Figure 10: Transaction tracking to view application performance..... 71
Figure 11: IBM Cloud APM Report - End User Transaction Performance..... 71
Figure 12: IBM Cloud - North America Data Centers 79

6. Technical Response

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

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

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

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

8 TECHNICAL REQUIREMENTS

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

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

8.1 (M)(E) TECHNICAL REQUIREMENTS

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

The cloud solution proposed by IBM as part of this RFP is in a full alignment with the NIST Special Publication 800-145. We provide Infrastructure (IaaS), Platform (PaaS), and Software (SaaS) Offerings, as needed to deploy, operate, and support the most challenging application portfolio, and to integrate with existing on premises legacy systems.

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

The five essential characteristics of the cloud model, as defined by NIST 800-145 are as follows:

- On-demand Self-Service:

Resources on the IaaS platform can be provisioned without human interaction from IBM.

- Broad Network Access.
- Resource Pooling.

- Rapid Elasticity.
- Measured Service.

The three service cloud models include the following:

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

The four cloud deployment models are as follows:

- Private cloud.
- Community cloud.
- Public cloud.
- Hybrid cloud.

The Sections below address in detail how each of the three service cloud models, as defined by the NIST 800-145, is satisfied by IBM cloud offering.

IaaS Response:

On-Demand Self-Service: Resources on the IaaS platform can be provisioned without human interaction from IBM.

Broad Network Access: IBM offers a variety of means for the clients to access the IBM Cloud Network resources, to include VPN, Direct Link, and others. For example:

IBM Direct Link connection (various options are available) provides the following features:

- Move data across a variety of connections, including 1Gbps and 10Gbps.
- Free and unmetered Local Routing.
- Optional global routing that provides access to out of region data centers.

VPN access to IBM Cloud infrastructure is enabled via the following ways:

- **SSL VPN:** Global access to our private network is quickly and easily accessed at a single URL, which redirects the client to the nearest VPN endpoint.
- **PPTP VPN:** Allows the client to securely connect to the private network using OS-specific client software from your desktop or on a dedicated device such as a firewall or router.
- **OPEN VPN:** Allows limited thin client OpenVPN connection (for the State to create proof of concepts)
- **Private Communication:** IPSEC VPN (VPNE) via the public interface, which is realized securely with IPSEC VPN Tunnel.

Resource Pooling: Consistent with the NIST 800-145 Standard Definition, resource pooling is the servicing of multiple clients from the same physical resources, by securely separating the resources on logical level.

The resource pooling strategy includes processing services, data storage services, and bandwidth provided services.

Through modern scalable systems involved in cloud computing and Software as a Service (SaaS), IBM's cloud can create a sense of immediately available resources by controlling resource adjustments at a Meta level. This allows the consumers to change their levels of service on demand without being subject to any of the limitations of physical or virtual resources. The isolation of multiple clients on IBM Cloud and allocation of Dedicated Resource pools facilitates no resource contention.

In a Public-with Dedicated Cloud Model, shown in the following figure, resources can be dedicated and the administrators can manage the catalog and policies, specify security policy, isolation, and integrity, and customize compute requirements.

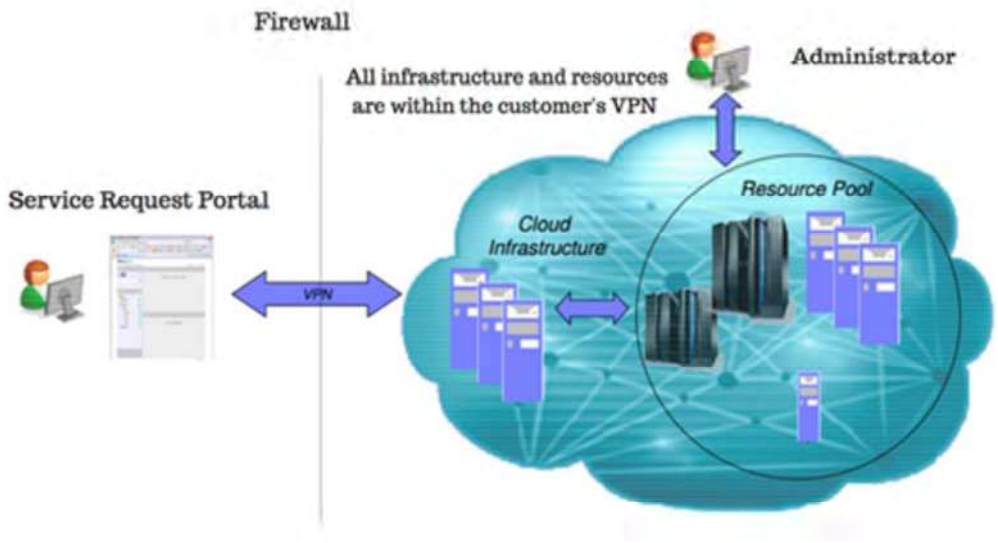

Figure 1: Resource Pool - Public Cloud - Dedicated Model

Rapid Elasticity: IBM Cloud enables the following two categories of elasticity:

- **Horizontal scalability:** Adding or removing nodes, servers, or instances to or from a pool, like a cluster or farm.
- **Vertical scalability:** Adding or removing resources to an existing node, server, or instance to increase the capacity of the node, server, or instance.

IBM Cloud provides the dynamic provisioning of services, and on demand self-service, where clients could change their levels of service without actually contacting IBM. This kind of automated service provisioning replaces traditional, labor-intensive strategies with new innovations that rely on increasingly powerful virtual networks and data handling resources. The client experience is isolated from the actual administration of cloud system assets, so that the process of delivery is transparent to the users and the services seem to be continuously available.

IBM Cloud provides Auto-Scaling capability, which automatically increases or decreases the compute capacity of a client's application. The number of application instances are adjusted dynamically based on the auto-scaling policy the client defines. Auto-Scaling offers the following two features:

- **Dynamic scaling:** Automatically add or remove resources to match the current workload.
- **Metric statistics:** Visualize the current and historical values of performance metrics.

The control over Auto-Scaling policies is available through the IBM Cloud API, which allows run time environments to scale up or down based on real-time workload performance and user-configured thresholds. The IBM Cloud provides versatile auto-scaling policies based on time, network throughput, CPU, and memory consumption. On the contrary, many other Cloud Service Providers provide auto-scaling primary of CPU resource.

Measured Service: IBM Cloud IaaS resources can be measured and monitored via a Customer Portal that includes detailed resources usage dashboard. The clients can monitor in real time computing resources consumption, and more. IBM Cloud's robust API can also feed client-side brokerage services and cloud management services, allowing monitoring via a familiar interface.

PaaS Response:

On-Demand Self-Service: Resources on the IaaS platform can be provisioned without human interaction from IBM.

Broad Network Access: PaaS is accessed over the network through internet browsers on a variety of platforms (laptop, workstation, mobile, and others).

Resource Pooling: IBM PaaS services run on IBM IaaS, the pooling characteristics that supports NIST Standard Definition 800-145 or the secure separation of multiple clients. IBM can also provide Dedicated Resource pools to make sure the resource pools are securely separated assuring no resource contention.

Rapid Elasticity: IBM Cloud enables the following two categories of elasticity:

- **Horizontal scalability:** Adding or removing nodes, servers, or instances to or from a pool, like a cluster or farm.
- **Vertical scalability:** Adding or removing resources to an existing node, server, or instance to increase the capacity of the node, server, or instance.

IBM Cloud provides the dynamic provisioning of services, and on demand self-service, where clients are able to change their levels of service without actually contacting IBM. This kind of automated service provisioning replaces traditional, labor-intensive strategies with new innovations that rely on increasingly powerful virtual networks and data handling resources. The client experience is isolated from the actual administration of cloud system assets, so that the process of delivery is transparent to the users and the services seem to be continuously available.

IBM Cloud provides Auto-Scaling capability, which automatically increases or decreases the compute capacity of a client's application. The number of application instances are adjusted dynamically based on the Auto-Scaling policy the client defines. Auto-Scaling offers the following two features:

- **Dynamic scaling:** Automatically add or remove resources to match the current workload.
- **Metric statistics:** Visualize the current and historical values of performance metrics.

The control over Auto-Scaling policies is available through the IBM Cloud API, which allows run time environments to scale up or down based on real-time workload performance and user-configured thresholds. The IBM Cloud provides versatile auto-scaling policies based on time, network throughput, CPU, and memory consumption. On the contrary, many other Cloud Service Providers provide Auto-Scaling primary of CPU resource.

Measured Service: IBM Cloud IaaS resources can be measured and monitored via a Customer Portal that includes detailed resources usage dashboard. The clients can monitor in real time computing resources consumption, and more.

SaaS Response:

IBM currently provides a portfolio of over 150 SaaS applications to our customers. These applications have different architectures, dependent upon the functionality that they provide. Regardless of architecture, these applications all conform to the NIST Characteristics as described.

Most IBM SaaS applications require initial provisioning by IBM Operations resources to establish service. Once the initial service has been established, additional users and business capabilities (functions) can be instantiated on-demand, by the customer. For some applications, this on-demand instantiation is extended to the initial provisioning of the service.

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

Yes, IBM is willing to comply with the requirements of Attachments C and D. Please refer to our Attachments C and D included in our submission package for examples of service offerings for each category.

The IBM Cloud organization has skills, technology, and capabilities to ensure the compliance with requirements included in the attachments referenced.

Our goal in responding to your Request is to identify service model sub-categories to assist you in best manners in matching your requirements. Therefore, we will include the most relevant and appropriate service model that shall best represent your point of view.

As requested by you, our key focus in this Response is on the services that include a mix of capabilities spanning service models. As an example, our services proposed to you include both IaaS capabilities for processing and storage with advanced PaaS capabilities for application deployment and DevOps operations support.

Also, as requested by you, we have identified and described our service offerings by Cloud Service Model (i.e. SaaS, IaaS or PaaS), including additional sub-categories and their descriptions. We have identified the most representative sub-categories and corresponding descriptions from the sample list provided by you in Attachment C – NIST Service Models.doc within at least one of the three Cloud Service Models (IaaS, PaaS and SaaS).

As concerned with the three Categories of Data Risk described in Attachment D: Scope of Services, we have IaaS Cloud offerings that support processing and storing the Low, Moderate, and High Data Risk in compliance with the most essential Industry Standards and Policies.

We will work very closely with you to understand your requirements with the goal to enable best Cloud solution infrastructure, as required to promptly handle any of the

three Data Risks indicated as part of the Cloud offerings that will be available for your operations on IBM Cloud.

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.

As described in Section 8.1.1 above in this document, our IaaS, PaaS, and SaaS cloud service models meet the five essential characteristics specified by the NIST 800-1454 to include **On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured service.**

IBM Cloud offerings and services consistently follow the definitions and nomenclature established as part of the NIST standards. IBM as one of the key leaders in cloud technology has to offer a rich portfolio of IaaS, PaaS, and SaaS offerings that address the most demanding requirements for migrating onto the cloud and operating on the cloud.

IBM IaaS, PaaS, and SaaS Cloud offering provides the infrastructure capability to store and secure one, all or combination of the Data that can be characterized as Low, Moderate and High Risk.

IBM has highly qualified and experienced resources that strive to provide an exceptional service to our clients. Our dedicated resources aim to take you on the journey to migrate and deploy your systems onto the cloud, and later to make sure you have your best experience as the consumer of cloud resources.

IBM will partner with you to implement continuous improvements and enhancements to your systems operated on IBM cloud as needed and to ensure a high satisfaction with our cloud offerings that we will provide to you as part of our agreement.

In addition, IBM provides Software as a Service (SaaS) Solutions in Public Cloud Environment. These are deployed in our Washington DC and Dallas FedRAMP Compliant data centers.

8.2 (E) SUBCONTRACTORS

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

IaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

PaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

SaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

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.

IaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

PaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

SaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

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.

IaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

PaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

SaaS Response:

IBM intends to deliver all components of the cloud solutions directly.

8.3 (E) WORKING WITH PURCHASING ENTITIES

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

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

IaaS Response:

IBM will follow IBM Computer Security Incident Response Team (CSIRT) procedures for any internal breach that impacts the IBM Cloud infrastructure and will notify our clients as appropriate following IBM CSIRT procedures, as required.

On IBM IaaS Cloud platform, IBM has no visibility into your workload(s) and has no role in handling security breaches on the State's workload (unless managed security services are contracted for separately). If necessary, IBM will support State

investigations. IBM regularly performs scans of the componentry supporting the management system as well as the perimeter network for access to clients subscribed compute resources.

Cloud services may be suspended if IBM reasonably determines that a security breach exists that affects your systems or the IBM infrastructure.

IBM will give reasonable advance notice of a suspension and an opportunity to remedy the cause of a suspension, unless immediate suspension is necessary to protect your systems, IBM, or any third party service providers from operational, security, or other risk, or is ordered by a court or other judicial body.

IBM will cooperate with the State and use our best effort to resolve issues in a timely manner. If managed services or managed security services have been contracted for, the SLAs for resolution will be described in those agreements.

IBM remediates any vulnerabilities encountered. A support and incident response team exists to notify our clients of items that require your attention or assistance or that are suspected of a breach. Only information required to allow the State to understand a potential exposure or that is needed for you to assist in a remediation will be shared with the State without disclosing information for other clients.

In keeping with best practices, periodic vulnerability assessment scans of provisioned instances with Nessus can be scheduled at no charge via the IBM Cloud portal. Remediation of any issues in user subscribed resources is the responsibility of the customer. Alternatively, the State can use their own utilities for vulnerability scans.

PaaS Response:

Same as IaaS. IBM PaaS has a security incident response plan that aligns with the IBM Cybersecurity Incident response process and the IBM Cybersecurity Incident Response team (CSIRT) is engaged wherever a suspected security incident involving a PaaS or client system or data.

SaaS Response:

Same as IaaS response.

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.

IaaS Response:

IBM will not, and does not, engage in pushing marketing adware or software vis-a-vis our client's relationship with IBM or IBM Cloud. IBM will not, and does not, sell or provide client data to third parties for marketing or any other purpose.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS response.

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

IaaS Response:

The IBM Cloud offering supports test/dev, pre-prod, UAT, and more environments that are identical to production. We provide comprehensive technology offerings, to include computing resources, storage, network, and network devices (firewalls, load balancers) and backup and recovery solutions, as needed to configure your cloud hosting environments consistently across development, test, and production.

While in the IaaS model, the clients are responsible for configuring cloud resources as needed to develop, test, and operate systems, IBM can provide comprehensive services to you to assist with the end to end environment architecture, design, and implementation as part of a separate DOU.

PaaS Response:

IBM supports test/dev, pre-prod, UAT, and more environments that are identical to production. IBM PaaS has segregated development, staging, and production environments deployed in different VLANs in different IaaS accounts. Each client environment is considered to be a production environment, but PaaS provides clients with the ability to deploy code into production and non-production spaces. It is the client's responsibility to restrict the movement of workload between their environments and make sure production data is not replicated to a non-production environment.

SaaS Response:

Similar to the above response for IaaS and in addition for SaaS applications, the testing environment is based on the business context of the application. For example, eCommerce applications may have a prototyping environment for new web functionality, BPM may allow for test of new processes. These are considered to be part of the production SaaS instantiation. Traditional staging and version testing of the application software is done on the SaaS application, by IBM, as part of the normal release management process.

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

IaaS Response:

IBM Cloud provides for accessibility requirements as needed by people with disabilities to access web sites hosted on IBM Cloud.

To enforce the IBM Cloud accessibility standards, IBM Cloud Organization directs teams to meet the relevant accessibility standards. Our accessibility standards are harmonized with several published international standards including:

- World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG 2.0) Level A & AA.
- U.S. Revised Section 508 standard.
- Europe EN 301 549 standard.
- Published on the web with guidance at IBM Accessibility Checklist.

IBM Cloud Offerings, Products, etc., are expected to perform Accessibility Verification Testing (AVT) as part of their design, development, and deployment process.

Since 2011, IBM products are required to meet the web accessibility checkpoints for WCAG 2.0 Level AA. This is in addition to meeting all previously required checkpoints relating to Section 508 and WCAG 2.0 Level A standards. To meet these guidelines, the Web Accessibility Initiative (WAI), a workgroup of the W3 Consortium, generated implementation requirements and best practices known as Accessible Rich Internet Applications (ARIA).

IBM Cloud includes the following major accessibility features:

- Keyboard-only operation.
- Operations that use a screen reader.

To take advantage of accessibility features, users utilize the latest release of their screen reader in combination with the latest Internet Explorer web browser that is supported by this product.

The IBM Cloud online product documentation and the IBM Cloud user interface framework is enabled for accessibility.

As part of continuous improvement to accessibility features, IBM Cloud offers an Automated Accessibility Tester, which is an experimental service allowing incorporation of automated accessibility reporting and auditing capabilities directly within your testing environment to quickly remediate accessibility violations before an application is deployed.

The Automated Accessibility Tester is intended to be used with test systems and test/staging data.

External customers, IBM Sales teams, etc., can request the latest accessibility conformance information about a specific offering from a publicly available IBM Cloud online resource. IBM's Accessibility Conformance Reports are published using ITI's Voluntary Product Accessibility Template (VPAT®) which is also required by the U.S. federal procurement process. The report includes a section for each of the applicable standards mentioned above. The U.S. Americans with Disabilities Act (ADA) does not specifically require a technical accessibility standard for information and communication but the conformance reports address all of the relevant requirements.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM has built integrated accessibility into our product development process. Completed accessibility checklists are required at key phases of the development process and accessibility verification is integrated into testing and validation procedures.

Below are just a few examples of our compliant product portfolio, which are capable – when used in accordance with IBM's associated documentation – of satisfying the applicable requirements of Section 508 of the Rehabilitation Act, provided that any assistive technology used with the product properly interoperates with it.

Accessibility features for people with disabilities:

- Support interfaces commonly used by screen readers.
- Can be operated using only the keyboard.
- Allow the user to request more time to complete timed responses.
- Support customization of display attributes such as color, contrast, and font size.
- Communicate all information independently of color.
- Support interfaces commonly used by screen magnifiers.
- Provide documentation in an accessible format.
- Support alternatives to audio information.
- Support adjustable volume control.

We can provide accessibility information about the IBM cloud offerings in this proposal, including Section 508 Voluntary Product Accessibility Templates (VPATs), upon request.

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

IaaS Response:

IBM Cloud supports current versions of the required browsers listed.

PaaS Response:

IBM Cloud supports current versions of the required browsers listed.

SaaS Response:

IBM Cloud supports current versions of the required browsers listed.

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.

IaaS Response:

IBM strictly complies with regulations regarding information, laws, and regulations, including sensitive and personal information within its span of control. To the extent that such information is in our systems as part of the IaaS/PaaS account(s) for the Purchasing Entity, the same would apply. In the context of this solicitation, at no time will IBM have access to the data in your environment; we will not use or store your data. IBM will never move your data, without an explicit request from you.

If required, we will plan on scheduling a meeting with interested parties to discuss privacy and data handling to define the strategy to handle sensitive or personal information that will be a subject of hosting on IBM Cloud platform.

Upon request, we will enter into additional agreements as required by law in the prescribed form for the protection of personal or regulated personal data included in the Content provided by you. We will agree that such additional agreement will be subject of the terms of the Agreement for the cloud services with you.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM provides over 150 SaaS applications. Some of these applications are capable of processing and storing SPI. Our services are designed to protect your proprietary content and data. We are committed to delivering best-of-breed privacy.

The data you own and upload into a SaaS offering remains yours.

We do not use your data for any reason except to deliver services and support to you.

Access to your data is only granted as necessary to deliver services and support to you (for example, least required privilege).

We are aligned with many industry and country requirements, while continuously monitoring regulatory environments for new requirements.

IBM will meet with your 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.

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.

IaaS Response:

IBM Cloud is designed to be completely self-service enabled, which allows our clients to implement solutions using their own development and implementation practices and their own resources. Should the State wish to engage IBM to help with solution implementations, IBM offers professional services that can be engaged to define cloud solutions. We have a large number of highly qualified project managers who are PMI certified, with an extensive experience in planning and delivering cloud-based solutions.

As part of the IBM Cloud solution implementation planning, the IBM project office identifies and documents the need for producing various project schedule plans and work plans that are later developed jointly with the customer and other third parties participating in the solution delivery.

A common example of a plan that is established for a Cloud Solution Delivery is an Integrated Delivery Plan (IDP). The IDP provides a single view of essential tasks owned by key project stakeholders, grouped by units of work with strict adherence to timeliness. The IDP includes task owners, phases, and milestones, and it maps to more granular plans that are concerned with various end-to-end solution components, activities, and phases that may include discovery, proof of concept, application migration, modernization, test planning and execution, component or application deployment, ongoing support and maintenance.

In parallel, a log of risks, issues, dependencies, and assumptions, as well as the RACI (Responsible, Accountable, Consulting, and Informed) matrix that clearly defines the roles of various parties in the solutioning process is maintained.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS response.

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.

IaaS Response:

IBM will maintain and update public instances of the Cloud Services on a regular basis during scheduled maintenance windows as published in support documentation available from the IBM Cloud UI.

IBM will deploy software updates to client's dedicated and local environments as scheduled in advance, with appropriate notification to the client, with the goal of keeping such environments reasonably current with the public instances.

IBM will provide the State with at least 30 days' notice in the IBM Cloud UI of any changes to service descriptions. Continued use of the cloud services after the effective date constitutes your acceptance of any changed pricing or terms. IBM may enable the State to continue to use existing instances of a withdrawn service during a transition period.

For those services identified as Tier 1 in the IBM Cloud UI, IBM will not withdraw the service without making a functional equivalent available or providing at least five years' notice of the withdrawal. If IBM disables or modifies an API, IBM will use commercially reasonable efforts to provide 1) advance notice of such change, and 2) continued support for prior versions of the API for a reasonable period of time, unless there are operational, legal, or security risks or burdens.

The IBM Cloud regular maintenance that should not require system downtime ("non-disruptive" maintenance) and maintenance that may require some system downtime and restarting ("disruptive" maintenance") will be performed at the scheduled times published in the IBM Cloud UI

Also, as shown in the Figure below, IBM Cloud UI provides the ability to view various types of Notifications, to include Incidents, Security, Maintenance and Announcements that you will have the access to as part the account with IBM Cloud.

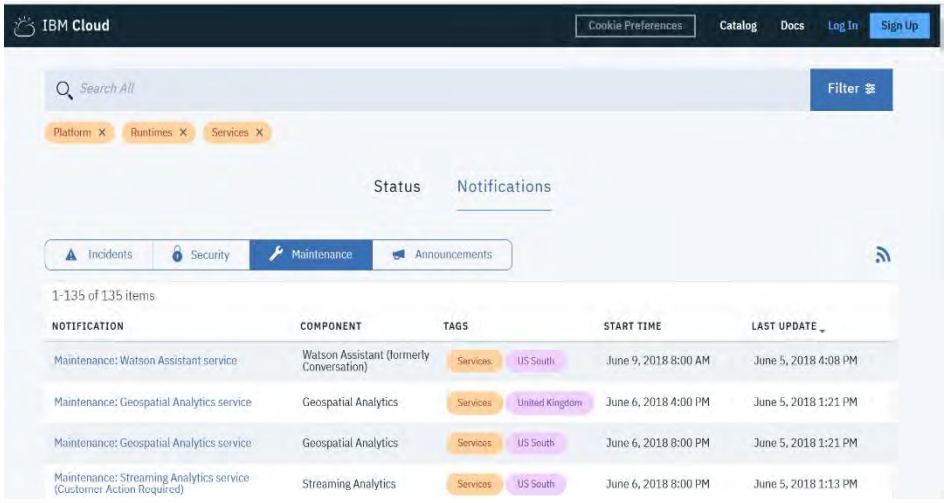

Figure 2: IBM Cloud UI - – Sample User Notifications

PaaS Response:

PaaS Public is done automatically and users are notified via notification subscription. PaaS Dedicated and IBM Cloud Private are done with client scheduled changes. Security Patches are highest priority and can affect SLAs, so those are mandatory.

Regular maintenance that should not require system downtime (“non-disruptive” maintenance) and maintenance that may require some system downtime and restarting (“disruptive” maintenance”) will be performed at the scheduled times published on the IBM Cloud developer support page.

SaaS Response:

IBM does continuously update our SaaS offerings. As part of our ISO 27001 and NIST 800 development, deployment and management compliance, we assess and ensure that functionality and security are not degraded. IBM contractually obligates ourselves to these requirements as part of our standard SaaS transaction documents.

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

  As with IBM's current NASPO Computer Equipment contract, IBM has a dedicated Contracts team that handles the administrative and support side of our contracts which includes, but not limited to, providing product updates/refreshes, handling reporting requirements, as well as contract administrative fee payments. This dedicated team also has responsibility for tracking and maintaining contract requirements, such as agreed upon contractual discount levels.

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

  IaaS Response:

  Any upgrades and technology changes as part of regular roadmap on the IBM public instances of the Cloud will be deployed on regular basis during scheduled maintenance windows that are published in cloud support documentation available from the IBM Cloud UI.

IBM will deploy software updates as per an established scheduled with appropriate advance notification to you. Our goal is to keep such environments reasonably current with the public instances. In circumstance of any major technology or service changes, IBM will provide the users with at least 30 days' notice in the IBM Cloud UI of any changes to service descriptions. Continued use of the cloud services after the effective date constitutes your acceptance of any changed pricing or terms. IBM may enable the users to continue to use existing instances of a withdrawn service during a transition period.

For those services identified as Tier 1 in the IBM Cloud UI, IBM will not withdraw the service without making a functional equivalent available or providing at least five years' notice of the withdrawal. If IBM disables or modifies an API, IBM will use commercially reasonable efforts to provide 1) advance notice of such change, and 2) continued support for prior versions of the API for a reasonable period of time, unless there are operational, legal, or security risks or burdens.

The IBM Cloud regular maintenance that should not require system downtime (“non-disruptive” maintenance) and maintenance that may require some system downtime and restarting (“disruptive” maintenance”) will be performed at the scheduled times published on the IBM Cloud developer support page.

PaaS Response:

Same as IaaS response.

SaaS Response:

Any upgrades and technology changes as part of regular roadmap on the IBM public instances of the Cloud will be deployed on regular basis during scheduled maintenance windows that are published in cloud support documentation available from the IBM Cloud UI.

IBM will deploy software updates as per an established scheduled with an appropriate advance notification to users.

IBM provides regular informational updates to its clients in its public documentation, regarding any updates or enhancements to its SaaS application.

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

IaaS Response:

Within the scope of this solicitation for self-service infrastructure and platform services, IBM provides extensive and efficient services and capability that allow the State to transition service with minimal disruption. IBM also has extensive best-in-class migration, professional, and managed services, should the Purchasing Entity elect to have IBM manage a transition on its behalf.

In circumstances of an intent to to discontinue or replace a generally available service IBM will provide at least 30 days notice. If an equivalent replacement is not provided for at least 12 months from the date of that announcement, IBM will use commercially reasonable means to continue the operation and support of previously deployed instances of the service.

PaaS Response:

IBM will provide at least 30 days' notice of its intention to discontinue or replace a generally available service. If an equivalent replacement is not provided for at least 12 months from the date of that announcement, IBM will use commercially reasonable means to continue the operation and support of previously deployed instances of the service.

SaaS Response:

IBM will provide at least 30 days' notice of its intention to discontinue or replace with a generally available service. IBM also provides instructional guides to assist clients in enacting any updates that may affect integrations with their internal systems. Further, IBM Customer Success Managers aid the client in the upgrade timing, where appropriate, and/or assist in linking IBM Lab Services with the Purchasing Entity's IT teams to ensure any project or enhancement activities are understood and planned appropriately.

8.4 (E) CUSTOMER SERVICE

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

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

IaaS Response:

IBM strives to provide best services to our client to facilitate satisfaction from our cloud offerings.

IBM Cloud Support includes the following Support Tiers:

Self Help, Basic, Advanced, and Premium.

The Basic, Advanced and Premium Support provide you with access to Technical Support teams 24x7 through online ticketing, phone, and chat.

The Basic Support is included with IBM Cloud billable accounts (Subscription of PayGo) at no charge. The Advanced and Premium Support are Fee based, and they both include Case escalation process, as needed to address urgent issues. They provide priority ticket handling with Response Time Objectives

In addition, as part of the Premium Support IBM Cloud can assign to the State a dedicated Technical Account Manager (TAM) who will assist you as needed to escalate any urgent requests for service. Premium Support also includes invitations to Cloud Insights sessions and Quarterly business reviews.

As part of our goal to provide you with the best available cloud experience, IBM Cloud provides the following SLAs for the key components of our Cloud infrastructure:

- Public Network: IBM Cloud will use reasonable efforts to provide a service level of 100% for the Public Network.
- Private Network: IBM Cloud will use reasonable efforts to meet a service level of 100% for the Private Network.

- Customer Portal: IBM Cloud will use reasonable efforts to meet a service level of 100% for access to the Customer Portal.
- Redundant Infrastructure: IBM Cloud will use reasonable efforts to meet a service level of 100% for access to the power and HVAC provided to you.

For the details of the IaaS services and SLAs provided by IBM Cloud please refer to the IBM Cloud Service Description document included in the IBM Appendix I IBM Cloud Service Descriptions Example_US.doc included with our submission. That document covers the following service areas:

- Cloud Service Usage.
- Set up and Maintenance.
- Network Access.
- Content and Data Protection.
- EU Supported Cloud.
- Service Level Agreements.
- Availability SLAs for the following:
  - Platform Services;
  - Infrastructure Services;
  - IBM Cloud Object Storage Offerings;
  - Infrastructure Hardware Replacement and Upgrade SLA.
- Technical Support.
- Charges.
- Subscription.
- Billing.

In addition, IBM Cloud IaaS's SLA are included in the SLA.PDF document available in IBM Appendix I IBM Cloud Service Descriptions Example_US.doc included with our submission, and also available on the IBM Cloud support website.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM customer service starts with our time-tested development, deployment, and operations processes which ensure that all of our SaaS customers encounter as few problems as possible. In the event that our customers have questions or issues, IBM employees a multi-level support strategy which escalates from self-service portals through direct development support.

Available at ibm.com, Our IBM Software as a Service (SaaS) Support Handbook details the support services, support resources, contact information, and best

practices for contacting Customer Support to help facilitate effective responses and issue resolution to our client's support needs.

Quality Assurance Measures: Satisfaction Surveys: We periodically survey customers to obtain additional feedback on recent experiences with Customer Support. The survey focuses on quality of support provided and overall experience. The survey results are reviewed by management. IBM reserves all rights, title and interest in and to any feedback that you provide to IBM, including without limitation, in the form of suggestions, ideas, concepts, improvements, reports and any other materials, whether written or oral.

Premium Support: The IBM Software Accelerated Value Program for SaaS ("AVP for SaaS") is an evolving suite of flexible and premium support services tailored to customers' needs and delivered on a recurring basis for an additional charge. The offerings include:

Client Advocacy: An assigned account manager who will work with you to gain an understanding of your business objectives and how the SaaS offering you purchased fits into your business eco-system. Your account manager acts as a point of contact and is your assigned advocate within IBM.

Technical Account Management: An assigned technical team or resource for technical consulting.

Business Support: An assigned team of product and industry experts who provide ongoing assistance to help you leverage the SaaS offerings to help you achieve your targeted business objectives.

Dedicated Business Support: An assigned product expert to supplement the needs of your team. Provides functional expertise for a particular area of your business.

Custom Support: Assigned resources to provide you with a level of support above our basic Customer Support model. This may include customized after hours support, language support, and response times.

Not all Premium Support offerings are available for all IBM SaaS offerings. The level of support, service and cost for premium support are defined in the customer's contract.

Escalation Plan: Severity levels are typically classified into four tiers, as an example; (1) Minimal business impact/functionality question - 1 day response, (2) Minor business impact/non critical function.

SLA: IBM SaaS SLAs vary based on application, and are focuses primarily on availability. In most cases, compensation for inability to meet service levels is based on a tiered scale, as an example; < 99% availability = 2% of monthly subscription, <97% = 5% of monthly subscription, <95% = 10% of monthly subscription. Note that IBM does provide 99.9% availability SLAs for some SaaS applications.

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.

IaaS Response:

Yes, IBM will comply with this requirement for our IaaS offerings.

PaaS Response:

Yes, IBM will comply with this requirement for our PaaS offerings.

SaaS Response:

Yes, IBM will comply with this requirement for our SaaS offerings.

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.

IaaS Response:

This requirement can be fulfilled through a support subscription.

As part of the Basic, Advanced, and Premium Support, the IBM Cloud Customer Service Representative are available 24x7 through online ticketing, phone, and chat.

IBM Cloud Support includes the following Support Tiers:

Self Help, Basic, Advanced, and Premium.

PaaS Response:

Same as IaaS response.

SaaS Response:

Hours of Operation

The Customer Support team is available to provide support via the following channels:

E-mail: Sunday 8:00 PM - Friday, 7:00 PM U.S. Central (excluding IBM company observed holidays).

Phone: Sunday 8:00 PM - Friday, 7:00 PM U.S. Central (excluding IBM company observed holidays).

Live Chat (for Business Support only): Sunday-Friday, 8:00 PM – 6:00 PM U.S. Central (excluding IBM Company observed holidays).

IBM Client Success Portal: 24 x 7

After Hours Support:

After Hours Support (outside of regular operating hours stated above) is available only for Severity 1 issues on business days/evenings, weekends and holidays.

To request After Hours Support, please call the support line for your country from the phone numbers listed above and follow the prompts.

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

IaaS Response:

This requirement can be fulfilled through an Advanced or Premium Support subscription.

IBM Cloud Support includes the following Support Tiers:

Self Help, Basic, Advanced, and Premium.

The Basic, Advanced, and Premium Support provide you with access to Technical Support teams 24x7 through online ticketing, phone and chat.

The Advanced Support provides the following request handling times:

- Severity 1: < 1 hour
- Severity 2: < 2 hours
- Severity 3: < 4 hours
- Severity 4: < 8 hours

The Premium Support provides the following request (ticket) handling times:

- Severity 1: < 1 hour
- Severity 2: < 1.5 hours
- Severity 3: < 2 hours
- Severity 4: < 4 hours

A dedicated Technical Account Manager is available for you as part of the Premium Support to handle any escalations.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM will comply with this requirement, reference above example (8.4.1) for levels of severity governing response times.

(Example) Service Request Workflow

Please contact Customer Support via one of the following channels: IBM Client Success Portal, email, chat, or phone.

Once your Support Portal ticket or e-mail is received, we review each item and assign a severity based on the issue details submitted. Each ticket is followed through to closure by Digital Analytics Customer Support personnel.

Chat: We will attempt to answer your business questions on chat. If you need technical assistance, please create a ticket via the portal or email. If we determine that we can better serve you by researching the questions while you are not waiting on chat, we will create a ticket from the chat to continue the investigation.

Phone: We will attempt to answer your questions on the phone. If we determine that we can better serve you by researching the questions while you are not waiting on the phone, we will create a ticket to continue the investigation.

IBM's SaaS support teams are available to assist with technical issues of varying degrees of severity. There may be occasions where the support teams may not be able to answer all your questions, but they will engage other groups within the company, including operations and/or development teams, to help provide answers to you.

Severity level guidelines and response time objectives

The following table outlines response time objectives that IBM strives* to achieve, measured from the time IBM receives your initial request for support, to the time IBM provides an initial communication back to you regarding your request.

Severity	Severity definition	Response time objectives	Response time coverage
1	Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution. **Note:** We will work with you 24 hours a day, seven days a week to resolve critical problems provided you have a technical resource available to work during those hours.	Within 1 hour	24×7
2	**Significant business impact:** A service, business feature, or function of the service is severely restricted in its use, or you are in jeopardy of missing business deadlines.	Within 2 business hours	Monday – Friday business hours
3	**Minor business impact:** The service or functionality is usable, and the issue does not represent a critical impact on operations.	Within 4 business hours	Monday – Friday business hours
4	**Minimal business impact:** An inquiry or non-technical request.	Within 1 business day	Monday – Friday business hours

**Please note: Response time objectives described in this document are intended to describe IBM's goals only, and do not represent a guarantee of performance.*

Customer responsibilities

You play a key role in assisting us when you have questions about or have encountered problems with your SaaS offering. Information that you provide about your system and/or problem is often critical to resolving your issue. The following practices can help our customer support team to better understand your problem and more effectively respond to your concerns, as well as help you make the best use of your time:

- Submitting problems electronically.

- Keeping different questions/issues separate (one problem per support ticket, incident or case).
- Selecting a Severity based on your judgment of the business impact.
- Keeping IBM support informed of major upgrades/implementations of your system (where applicable).
- Providing timely feedback on recommendations, so the customer support team can close out the support ticket when the problem has been resolved. If the problem reoccurs you may reopen the original support ticket by resubmitting it electronically.

You will be required to provide the following information when contacting support:

- Your name, company name, email address, and telephone number with extension (if applicable).
- Ticket, incident, or support case number (as applicable).
- Support entitlement identifiers such as client ID, mailbox ID, or IBM customer number, as appropriate for the offering.
- Product name (release level and any product maintenance level, if applicable).
- Any additional information required by the customer support team.

Premium support

The IBM Software Accelerated Value Program for SaaS (“AVP for SaaS”) is an evolving suite of flexible and premium support services tailored to customers’ needs and delivered on a recurring basis for an additional charge. The offerings include:

1. Client advocacy: An assigned account manager who will work with you to gain an understanding of your business objectives and how the SaaS offering you purchased fits into your business eco-system. Your account manager acts as a point of contact and is your assigned advocate within IBM.
2. Technical account management: An assigned technical team or resource for technical consulting.
3. Business support: An assigned team of product and industry experts who provide ongoing assistance to help you leverage the SaaS offerings to help you achieve your targeted business objectives.

   Dedicated business support: An assigned product expert to supplement the needs of your team. Provides functional expertise for a particular area of your business.
4. Custom support: Assigned resources to provide you with a level of support above our basic customer support model. This may include customized after hours support, language support, and response times.

Not all premium support offerings are available for all IBM SaaS offerings. The level of support, service and cost for premium support are defined in the customer’s contract.

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

IaaS Response:

IBM has highly skilled resources as needed to plan, architect, design, implement, and operate your applications on our Cloud platform.

We can assist you in designing the end-to-end infrastructure required to deploy your applications on the cloud, to include computing resources, network, storage, backup and recovery solution.

As part of the design process, our Cloud Subject Matter Experts can recommend the best configuration for cloud resources, as needed to optimize your cloud hosting environment, and in result, lower the overall cost of operating your assets on the cloud.

One of our key services is **IBM Cloud Garage** which is IBM's consultancy with a startup DNA. IBM Cloud Garage empowers small and large companies to rapidly identify, design, prove, and build the right innovative, scalable applications on IBM Cloud for the client's target market. The Garage helps to build modern hybrid cloud platforms and enables and trains the client to adopt cloud solutions.

While we are capable of providing the best in class design services using our internal resources, to give your more choices, IBM Cloud provides an online overview of its partner catalog of MSPs and consultants. IBM provides an on-line registry of IBM Cloud Business Partners that is accessible at IBM Partner World website (publicly available).

Project-specific consulting, implementation or managed service consulting will require a separate statement of work (SOW) to complement IBM Cloud services.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM provides design services for our SaaS applications. Dependent on the nature of the application and the scope of the design services, this may be either free or at additional cost to the customer.

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

IaaS Response:

IBM will provide you with our highly qualified Subject Matter Experts to perform installation services required to migrate or deploy your applications on our cloud platform for any of the offerings described in this RFP Response document.

We will work with you to identify the installation services you may need to deploy your systems on the IBM Cloud, or to consume cloud-hosted resources, and we will secure our service through a Document of Understanding (DOU) for the selected services that we will benefit your cloud strategy.

The following are the examples of installation services that you can invoke in automated manner directly from the IBM Cloud User Interface:

- You can provision bare metal servers in IBM Cloud data centers around the world in two to four hours. If you need to be online in minutes or only need

limited resources, you can select an hourly bare metal server. The fully automated process will deploy the servers for you on IBM Cloud.

- You can deploy IBM Cloud Virtual Servers in a matter of minutes. The virtual servers are deployed from your choice of virtual server images and in the geographic region that makes sense for your workloads.
- IBM Cloud has established a broad portfolio of Managed Services to address our customers' needed in various cloud operations domains.
- IBM Cloud Migration Services provides full or assisted migration of systems to the IBM Cloud.
- IBM Cloud engineers can assist you to design and create your network infrastructures on the IBM Cloud.
- IBM's Cloud Application Innovation service line can perform an implementation of cloud-native solutions not only on IBM Cloud but also on AWS, Azure, Google Cloud Platform and other common cloud service provider platforms.

PaaS Response:

PaaS services are self-service and available on demand. Project-specific consulting, implementation, or managed service consulting will require a separate statement of work to complement IBM Cloud services.

SaaS Response:

Typically, installation services are not required, or are encompassed through the initial provisioning of the SaaS application. These installation services are normally considered to be part of the SaaS cost. Installation Services which Purchasing Entity may require that are additional to SaaS Implementation included in the quotation(s), may be contracted directly with IBM under a separate quotation or SOW.

8.5 (E) SECURITY OF INFORMATION

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

IaaS Response:

Infrastructure (IaaS) and Platform (SaaS) Services are self-managed by the State, including selection of available data centers and selection, configuration, and management of services (such as security, backup, failover, restore, and monitoring), which the State determines are necessary to meet your requirements and applicable laws, including data protection and other regulatory requirements for its workloads and content.

To protect your data in any circumstances, we make available IBM Multi-Cloud Data Encryption that prevents the data misuse whether it resides in single cloud, multiple clouds, or hybrid environments. It encrypts file and volume data while maintaining access control. Finally, IBM Multi-Cloud Data Encryption helps you meet government and industry compliance regulations, such as PCI, GDPR, and more.

As IBM Cloud provides broad spectrum of data processing and storing technologies, the measure and technology to hold and protect your data may vary.

Just to provide a few examples, your retained at-rest data on IBM Cloud will be protected as follows:

- Encryption for data at-rest using AES 256 is currently available in several IBM Cloud data centers.
- IBM Cloud for VMWare Solutions provides Geo-fencing and encryption from HyTrust.
- VMware vCenter Server on IBM Cloud provides storage with data encryption at-rest.
- Block and File storage provide at-rest data encryption: Disk level with provider managed keys.
- IBM Cloud Backup eVault (multi-tenant environment) service provides in-transit and at-rest data encryption.
- IBM Cloud Back up R1Soft (single-tenant) service provides data encryption and compression.

The data processing and protection data sheet (Data Sheet) provides information specific to the cloud services regarding the type of content enabled to be processed, the processing activities involved, the data protection features, and specifics on retention and return of content. Any details or clarifications and terms, including the State's responsibilities around use of a cloud service and data protection features if any, are set forth in that document or they may be provided in additional data sheets as necessary.

There may be more than one data sheet applicable to the State's use of the cloud services based upon services and options selected by the State. Data sheets for each cloud service are made available through the IBM Cloud UI, and the additional data sheets may be only available in English and not available in local languages. Despite any practices of local law or custom, the parties agree that they understand English and it is an appropriate language regarding acquisition and use of the cloud services.

Unless IBM Managed Services are engaged as part of a separate DOU with you, as a consumer of IBM Cloud IaaS and PaaS platforms, the State is responsible to take necessary actions to order, enable, or use available data protection features for a cloud service and accepts responsibility for use of the cloud services if the State fails to take such actions, including meeting any data protection or other legal requirements regarding content. IBM's Data Processing Addendum (DPA) applies and is referenced as part of the agreement, if and to the extent the European General Data Protection Regulation (EU/2016/679) (GDPR) applies to personal data contained in content. The applicable data sheets for this cloud service will serve as the DPA exhibit.

IBM Cloud IaaS employs a decommissioning and reclaim process for hardware being reclaimed. The reclaimed drive is wiped using the DOD 5220.22-M algorithms. If a device is determined to be end of life, the hardware is wiped using the same method described above and the device is physically crushed onsite. These measures are taken to protect the State's data. (ISO27001 A.8)

In case of exiting the service agreement, IBM Cloud employs a procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a client has exited our environment or has vacated a resource. The IBM Cloud IaaS sanitization procedure is public facing and available to the State upon request. The IBM Cloud IaaS client service agreement documents the process for exiting the service arrangement.

PaaS Response:

Platform and Infrastructure Services are self-managed by the State, including selection of available data centers and selection, configuration, and management of services (such as security, backup, failover, restore, and monitoring), which the State determines are necessary to meet your requirements and applicable laws, including data protection and other regulatory requirements for its workloads and content.

Data-at-rest encryption for a PaaS application's data is the responsibility of the application developer, and they can use services provided by IBM PaaS to backup data – see details under the Cloud Data Services section of the PaaS services catalog.

IBM PaaS platform data is encrypted in transit. Data-in-transit encryption uses TLS from internet to the reverse proxy at edge of the PaaS network, which terminates TLS. IPSEC-based encryption is provided within the PaaS network for data-in-transit from the reverse proxy to PaaS components. IBM PaaS clients must make sure their applications are TLS enabled. Custom certifications can be associated with the PaaS application endpoints using the UI.

The process outlined in DSI07.1 is followed for any service being cancelled in IBM PaaS.

SaaS Response:

The following are samples of some of the key methods we use to protect your data within our SaaS offerings:

Compartmentalization:

Compartmentalization is the act of limiting access, whether physical or logical, to those personnel who genuinely need it to perform their jobs. IBM limits authorized physical access to data centers, for example, to personnel with a business reason to be there. (In fact the vast majority of IBM employees have no physical access to any data center.) IBM also limits authorized logical access to applications and databases, for example, to personnel whose job function requires it. Compartmentalization is a technique that helps control risks associated with accidental or intentional human behavior.

Least Privilege:

The Principle of Least Privilege says that personnel who need some kind of access should have the least amount of access necessary to perform their job function. This principle is applied both physically and logically. For example, just because someone needs access to one network control center to perform their job function does not mean they need access to every network control center. The principle is applied to logical controls as well. For example, those who need log on privileges to a certain server are not given highest privilege (“superuser” or the equivalent) unless that is also required for their job function.

Separation of Duties:

Separation of Duties is the principle of checks and balances. For example, an IBM person who administers a particular database should not be the same person who audits the security procedures for that database. Separate people or groups exist to check on each other. This limits the temptation to relax security procedures. IBM practices extensive separation of duties. For example, the software area business controls team is independent from any of the organizations they audit.

Defense in Depth:

Defense in Depth refers to the practice of creating multiple layers of security. Instead of a simple physical or logical block, beyond which there is free rein, multiple blocks are placed in succession, like layers of an onion. The layered approach to security helps prevent many types of attacks from being carried out. A failed block in one place is essentially backed up by other blocks. An example of physical defense in depth is requiring badge access to a building, then also badge access to a data center and then also maintaining separate access control to server cages within the data center. This creates three layers of security. Site access adds a fourth layer and there can be more.

Continuous Improvement by Design:

Business controls are designed to be improved as time goes on and conditions change. They have expirations or re-approval dates. For example, this Core Practice is revalidated at least annually. During revalidation, the Core Practice is examined in light of any changes that have occurred and adjusted accordingly. The Core Practice itself requires that it be reexamined and improved (see title page for current Core Practice revalidation status).

IT Risk Management:

Risk assessment and risk management are fundamental foundations of data security.

For IBM, there is an IT Risk Management Steering Committee headed by the IBM CIO. Members of the committee are security professionals, executives, and people who create internal IT standards for management approval. The function of this committee is to continually examine IT risks across a broad spectrum of potential threats. The output of this committee is used to improve IBM's IT risk posture. Our internal business controls staff periodically audits for compliance (for example, integrated into business controls).

Media and Physical Disposal of Media:

Only approved carriers are used to transfer electronic media that may contain unencrypted data. Server media used for backup, records retention, or DR is required to be physically protected against unauthorized use, theft, and damage.

Server storage Media Custodian handling Customer Data are responsible for accurate media inventory and for reporting any discrepancies according to and using IBM's Security Incident Handling Process (SIHP). In keeping with the separation of duties security principle, at least one person not involved in the media operation must perform the inventory (the Storage Media Custodian may participate, but is not permitted to be solely responsible for performing the inventory).

Physical media received from customers is handled separately from IBM data, but is also inventoried and handled in a controlled manner. Records are kept concerning its

lifecycle from being shipped to IBM to its being disposed of, either returned or destroyed.

Media, storage devices, and computing devices being returned to an IBM asset center must be “wiped” to render the data unreadable before shipment.

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

IaaS Response:

Protecting your data is mission critical to IBM Cloud and it is a shared responsibility between IBM and the State. IBM services are designed to protect your proprietary content and data. IBM provides comprehensive facilities and services which allow you to strictly control access to data and monitor access. This in accordance with IBM’s internal privileged user monitoring and auditing programs, and as described in Section 8.5.3.

IBM was one of the first companies to appoint a Chief Privacy Officer to develop and publish a genetics privacy policy, to be certified under the APEC Cross Borders Privacy Rules system, and to sign the EU Data Protection Code of Conduct for Cloud Service Providers.

We work with independent auditors and third party organizations to meet the industry’s most stringent guidelines. IaaS certifications, as concerned with the data privacy and security that include the following:

FISMA, FedRAMP, (NIST 800-53 included) FFIEC, SOC reports, ISO 27001, ISO 27017, ISO 27018, Cloud Security Alliance (Star) Level 1, PCI Compliance, HIPAA, HITRUST Assessment, GSMA (DAL09, PAR01), CJIS Standards, EU Model Clauses, Privacy Shield, IBM ISO Management System Certifications. IBM also complies with GDPR.

IBM Cloud compliance website (publicly available) provides very detailed listing of certifications and corresponding details.

PaaS Response:

We adhere to IBM security standards across the IBM Cloud portfolio, which are intended to comply with applicable regulatory regimes.

We work with independent auditors and third-party organizations to meet the industry’s most stringent guidelines. PaaS certification includes the following:

ISO 27001, ISO 27017, ISO 27018, SOC 1 Type 2, SOC 2 Type 2, CSA Star Level 1, Privacy Shield, and EU Model Clauses.

IBM also complies with GDPR.

The IBM Dedicated PaaS has the above certifications plus PCI and HIPAA.

SaaS Response:

Our services are designed to protect your proprietary content and data. We are committed to delivering best-of-breed privacy.

The data you own and upload into a SaaS offering remains yours.

We do not use your data for any reason except to deliver services and support to you.

Access to your data is only granted as necessary to deliver services and support to you (for example, least required privilege).

We are aligned with many industry and country requirements, while continuously monitoring regulatory environments for new requirements. IBM also complies with GDPR.

We will use your contact information according to, as applicable, IBM's Privacy Policy, the IBM Software Products and SaaS Privacy Statement, and the terms and conditions to your SaaS offering, and as needed to support you and keep you informed on updates related to your services.

For information on IBM's conduct of the company with respect to privacy and security, please see the Privacy & Security portion of the Governance section of IBM's 2013 Corporate Responsibility Report.

Please refer to 'IBM Security & Privacy Principles for SaaS' in question 6.7 for additional detail.

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.

IaaS Response:

IBM Cloud personnel does not have access, and will not access user accounts or data. IBM will not access, modify, delete, or retain client data, unless specifically requested by you and clearly defined in the DOU.

Unless managed or professional services are contracted for separately, IBM will never have access to, touch, or move the Purchasing Entity's data. The same applies to user accounts. If such services are contracted for, the applicable SOW and contracts will describe responsibilities for your data and user accounts.

PaaS Response:

Same as IaaS response.

SaaS Response:

Our services are designed to protect your proprietary content and data. We are committed to delivering best-of-breed privacy.

The data you own and upload into a SaaS offering remains yours.

We do not use your data for any reason except to deliver services and support to you.

Access to your data is only granted as necessary to deliver services and support to you (i.e., least required privilege).

We are aligned with many industry and country requirements, while continuously monitoring regulatory environments for new requirements.

We will use your contact information according to, as applicable, IBM's Privacy Policy, the IBM Software Products and SaaS Privacy Statement, and the terms and conditions to your SaaS offering, and as needed to support you and keep you informed on updates related to your services.

For information on IBM's conduct of the company with respect to privacy and security, please see the Privacy & Security portion of the Governance section of IBM's 2013 Corporate Responsibility Report.

Please refer to 'IBM Security & Privacy Principles for SaaS' in question 6.7 for additional detail.

8.6 (E) PRIVACY AND SECURITY

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

IaaS Response:

IBM is fully committed to comply with NIST standards, and as such, all IBM Cloud supports the five essential characteristics, three services models and four deployment models, as defined by NIST 800-145. We provide latest technology, services, and expertise needed to handle various data types that will be hosted on our Cloud platform.

IBM Cloud commercial data centers are managed to IBM Cloud security policies, based on NIST 800-53 and 800-145 frameworks.

Further, all IBM Cloud data centers are audited to SOC2 Trust Security Principles as evaluated in the third party SOC2 Type II assessment. Note that because all data centers are managed to the same policy and are audited for effectiveness of controls with SOC2, all commercial data centers are managed to FISMA standards (but not all are audited / assessed to FISMA - largely a logistics and cost issue due to requirement that each data center be physically audited for FISMA).

IBM Cloud works with independent auditors and third party organizations to comply with the industry's most stringent guidelines. IaaS certification include the following:

FISMA, FedRAMP, FFIEC, SOC reports, ISO 27001, ISO 27017, ISO 27018, Cloud Security Alliance, PCI Compliance, HIPAA, HITRUST Assessment, GSMA (DAL09, PAR01), CJIS Standards, EU Model Clauses, Privacy Shield, IBM ISO Management System Certifications.

The detailed information and the copies of the certificates are available at the IBM Cloud compliance website.

In addition, IBM has purpose built data centers for FedRAMP workloads. These data centers are reserved for government workloads and are assessed to both FISMA and FedRAMP standards.

IBM Cloud IaaS security controls are maintained through frequent internal audits and are validated by external auditors through assessments including, but not limited to, FedRAMP, ISO27001, SOC, PCI, and HIPAA. That demonstrates our commitment to secure and support different types of data we may receive from the State as part of hosting your systems or data repositories on IBM Cloud infrastructure.

PaaS Response:

IBM is fully committed to comply with NIST standards, and as such, all IBM Cloud supports the five essential characteristics, three services models and four deployment models, as defined by NIST 800-145. We provide latest technology, services, and

expertise needed to handle various data types that will be hosted on our Cloud platform.

We work with independent auditors and third-party organizations to meet the industry's most stringent guidelines. PaaS certification includes the following:

ISO 27001, ISO 27017, ISO 27018, SOC 1 Type 2, SOC 2 Type 2, CSA Star Level 1, Privacy Shield, EU Model Clauses.

The IBM Dedicated PaaS has the above certifications, plus PCI and HIPAA.

SaaS Response:

IBM has implemented many of its Privacy & Security Policies and Procedures informed and aligned with the corresponding NIST criteria. In addition, IBM has chosen the ISO27001 as the primary Security & Privacy Standard, by which, it will certify all of our SaaS Offerings. The ISO Standard is regarded as a covering enhancement to NIST. In addition to function specific Certifications, all IBM SaaS Offerings, without exception, are required to be certified to ISO 27001 by an independent third party.

All current IBM SaaS offerings are compliant with ISO27001.

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.

IaaS Response:

The IBM Cloud infrastructure's information security policies and security management approach is aligned with US standards and based on NIST 800-53 framework. IBM Cloud has the following compliance and certification standards:

SOC 1, SOC 2, SOC 3, ISO 27001, ISO/IEC 27017, ISO/IEC 27018, EU Model Clauses, HIPAA, PCI DSS 3.1, FedRAMP, FDA GxP, ITAR

IBM Cloud for Government is certified for FISMA Moderate and NIST 800-53, CJIS, DoD DISA Level 2, SOC 1, SOC 2, SOC 3, ISO/IEC 27017, ISO/IEC 27018, CSA Star Level 1, EU Model Clauses, Privacy Shield, HIPAA, HITRUST CSF, GxP-FDA, PCI-DSS Level 1.

In addition, IBM Cloud infrastructure supports clients and financial workloads through its policies and procedures. IBM engaged an independent audit to perform a controls assessment based on COBIT methodology to provide evidence of IBM Cloud infrastructure's suitability for financial services workloads:

- Received satisfactory rating.
- Approach was based on IT Governance Institute (ITGI) COBIT methodology as the preferred standard for financial institutions regulated by the Sarbanes Oxley Act (SOX).

IBM Cloud infrastructure is suited to host financial services, including FFIEC:

- Clients may choose to host their multi-tenant workload on the single tenant IBM Cloud Bare Metal Servers or IBM Cloud Virtual Servers (Private) cloud.

- While IBM Cloud Virtual Servers (Public) are suitable for regulated workloads, we recommend single tenant models in cases where an extra layer of protection is sought.

The detailed information on the security certifications IBM Cloud holds and copies of certificates are available at the IBM Standards Compliance website (publicly available).

PaaS Response:

We work with independent auditors and third party organizations to meet the industry's most stringent guidelines. PaaS certification includes the following:

ISO 27001, ISO 27017, ISO 27018, SOC 1 Type 2, SOC 2 Type 2, CSA Star Level 1, Privacy Shield, EU Model Clauses.

The IBM Dedicated PaaS has the above certifications plus PCI and HIPAA.

SaaS Response:

- All SaaS applications are Compliant with ISO27001 and have third party Certifications.
- ISO 27017 and 27018 are applicable where stated in the Service Description. Additional Standards (such as those below) are also available in those SaaS offerings where stated in their respective Service Descriptions. HIPAA where appropriate based on application functionality.
- HIPAA where appropriate based on application functionality.
- PCI-DSS where appropriate based on application functionality.
- FISMA where appropriate based on application functionality / Government usage.
- FFIEC where appropriate based on application functionality.
- FedRAMP where appropriate based on application functionality / Government usage.
- Additional Standards have been mapped to corresponding ISO 27001 Annex A Controls.

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

IaaS Response:

IBM has nearly 60 Cloud Data Centers in six regions and 18 availability zones, and IBM Cloud has implemented extensive measures to include physical protection of our cloud computing infrastructure, to secure the assets we host. These measures include:

- Every IBM Cloud Data Center is built to prevent physical intrusion, and server rooms are only accessible to certified employees.
- Physical security parameters can include fences, walls, barriers, security guards, gates, electronic surveillance, video surveillance, physical authentication mechanisms, reception desks, security patrols, and more.

- The controls deployed at IBM data centers are in compliance with standards, such as NIST 800-53 PE and ISO27001 A11, and they have been certified by an external auditor. Every IBM Cloud service is designed, developed and managed according to IBM's own strict security policies and implementation guidelines, and provided to you under the binding commitments of the IBM Data Security and Privacy Principles contained in IBM Appendix VIII Data Security and Privacy Principles - Z126-7745-WW-3_05-2018_en_US.pdf which has been submitted with our response.
- IBM Cloud IaaS restricts access to information and application system functions in accordance to the NIST 800-53 standard with the Logical Access Control Policy and related procedures.
- IBM Cloud IaaS's Data Security Architecture is designed using industry standards and best practices based on NIST 800-53.
- The IBM Cloud IaaS Security Operations Center routinely scans internal and external facing non-client apps for vulnerabilities. The Security Operations Center reports discovered vulnerabilities to the appropriate system owners for remediation in accordance with applicable standards.
- IBM Cloud IaaS engages third party groups as well as IBM to conduct penetration testing as prescribed by industry best practices.
- The IBM Cloud API provides the ability to perform application vulnerability scanning, data encryption, SSL termination, and a variety of other security controls as needed to secure the network access, data, and applications. It monitors that these security controls are appropriately applied to facilitate full compliance with security controls and security practices.
- We provide data encryption technologies, as needed to secure the most critical data that are processed and stored on IBM Cloud infrastructure. IBM Cloud IaaS employs logical segmentation in all networks and the hypervisors enforce compute isolation in Virtual Machines. These controls are tested regularly by penetration tests.
- The IBM Cloud provides security features that extend beyond FedRAMP controls in its ability to shore up Intel Trusted Execution Technology (TXT) and HyTrust that enable the ability for our customers to provision physically isolated private clouds within the IBM Cloud fabric, not merely virtual private clouds that only rely on 'virtual' isolation from other tenants.

PaaS Response:

IBM data centers are secured with server-room access limited to certified employees. Physical security parameters can include fences, walls, barriers, security guards, gates, electronic surveillance, video surveillance, physical authentication mechanisms, reception desks, security patrols, and more. The controls have been certified by an external auditor.

See NIST 800-53 PE and ISO27001 A11 for the relevant controls.

SaaS Response:

IBM employs access control mechanisms to limit access to system assets and infrastructure components. Keys, cipher locks, electronic controlled access systems,

guarded entrances, and in some cases biometric controls are all examples of physical access control employed by IBM.

IBM is recognized as trusted by our customers based on a legacy of leadership of our tools in the IT Security Marketplace Customers reasonably need some validation and security of IBMs policies and controls which is why, IBM has made this public commitment on our SaaS offerings on our ibm.com Trust site.

All IBM SaaS applications are currently compliant with ISO27001.

Furthermore, recognizing a customer's needs verifications IBM is voluntarily undergoing ISO 27001:2013 Certification for all SaaS offerings with independent third party auditors to validate and confirm IBM security and privacy controls.

ISO 27001 is an internationally recognized set of Information Security standards and controls including

- Information security policies (2 controls).
- Organization of information security (7 controls).
- Human resource security - 6 controls that are applied before, during, or after employment.
- Asset management (10 controls).
- Access control (14 controls).
- Cryptography (2 controls).
- Physical and environmental security (15 controls).
- Operations security (14 controls).
- Communications security (7 controls).
- System acquisition, development and maintenance (13 controls).
- Supplier relationships (5 controls).
- Information security incident management (7 controls).
- Information security aspects of business continuity management (4 controls).
- Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls).

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).

IaaS Response:

Within the scope of this solicitation, IBM does not have access to the State's data. At no time would your data ever be on an IBM laptop, mobile device, and removable media; there is no removable media facility in IBM Cloud data centers and removable media, personal devices are forbidden by policy in IBM Cloud Data centers.

IBM has a long history of providing successful data protection services to our customers. If the IBM Cloud Organization is engaged to manage a customers' information and data as part of Managed Services secured as part of a separate DOU (as indicated in Section 8.5.2 above in this document), our top mission is to provide the best protection to ensure the confidentially and integrity of your data.

Our practices assure that the access to your data is strictly controlled and monitored in accordance with IBM's internal privileged user monitoring and auditing programs.

IBM Cloud secure data management operations follow the best industry practices, and we have obtained several compliance certifications proving our commitment to standards, such as ISO 27001 (outlining the requirements for information-security management systems and provides a systematic approach to managing company and customer information based on periodic risk assessments.), 27017 (guidelines for information-security controls applicable to the provisioning and use of cloud services) and 27018 (PII protection).

The standards referenced are widely-adopted global security standards outlining the requirements for information-security management systems and they provide a systematic approach to managing company and customer information based on periodic risk assessments.

IBM Cloud complies with General Data Protection Regulations (GDPR). HyTrust, Intel and IBM Cloud jointly have established a Single Solution for Simplifying GDPR Compliance. HyTrust workload security solutions on IBM Cloud platform reduce data security risks by automating compliance and enforcing security-based policies across private and public clouds. As an integral part of IBM Cloud Secure Virtualization, HyTrust helps removing the security and compliance barriers that often prevent companies from accelerating their cloud adoption.

We work with independent auditors and third party organizations to meet the industry's most stringent guidelines. IaaS certifications, as concerned with the data privacy and security that include the following:

FISMA, FedRAMP, (NIST 800-53 included) FFIEC, SOC reports, ISO 27001, ISO 27017, ISO 27018, Cloud Security Alliance (Star) Level 1, PCI Compliance, HIPAA, HITRUST Assessment, GSMA (DAL09, PAR01), CJIS Standards, EU Model Clauses, Privacy Shield, IBM ISO Management System Certifications.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS response.

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.

IaaS Response:

The IBM Cloud infrastructure's information security policies and security management approach is aligned with US standards and it is based on the NIST framework. It has the following certifications that confirm compliance with industry standards:

SOC 1, SOC 2, SOC 3, ISO 27001, ISO/IEC 27017, ISO/IEC 27018, EU Model Clauses, HIPAA, PCI DSS 3.1, FedRAMP, FDA GxP, ITAR.

IBM Cloud for Government is certified for FISMA Moderate and NIST 800-53, CJIS, DoD DISA Level 2, SOC 1, SOC 2, SOC 3, ISO/IEC 27017, ISO/IEC 27018, CSA Star Level 1, EU Model Clauses, Privacy Shield, HIPAA, HITRUST CSF, GxP-FDA, PCI-DSS Level 1.

IBM Cloud Platform uses external auditors to conduct multiple structured, industry standard audit assertions and reports. For our latest security profile, please refer to our publicly available website.

PaaS Response:

We adhere to IBM security standards across the IBM Cloud portfolio.

We work with independent auditors and third-party organizations to meet the industry's most stringent guidelines. PaaS certification includes the following:

ISO 27001, ISO 27017, ISO 27018, SOC 1 Type 2, SOC 2 Type 2, CSA Star Level 1, Privacy Shield, EU Model Clauses.

The IBM Dedicated PaaS has the above certifications plus PCI and HIPAA.

For our latest security profile, please refer to our publicly available website.

SaaS Response:

- All SaaS applications are Compliant with ISO27001. Third party Certification of all applications is anticipated to be by the end of 2016 (many are already Certified).
- Future plans for 27017 and 27018 Compliance.
- HIPAA where appropriate based on application functionality.
- PCI-DSS where appropriate based on application functionality.
- FISMA where appropriate based on application functionality / Government usage.
- FFIEC where appropriate based on application functionality.
- FedRAMP where appropriate based on application functionality / Government usage.
- Additional Standards have been mapped to corresponding ISO 27001 Annex A Controls.

For our latest security profile, please refer to our publicly available website.

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.

IaaS Response:

IBM enforces logging and monitoring of actions taken by IBM privileged admins. To the extent that these actions may impact the State, they are available to you through your service tickets and the device management history viewable through the web portal and API.

IBM provides audit logs for authentication and portal/API driven actions taken by the State's users.

The State is responsible for auditing all operating system and above-level access to their servers.

IBM Cloud IaaS processes around Audit Logging and Intrusion detection are developed based on the NIST 800-53. Audit logs are stored and retained to FISMA standards. These logs are protected by active directory user credentials and physical access controls with all access and actions logged and monitored.

IBM Cloud Activity Tracker tracks how applications and users interact with the IBM Cloud services. Customers can use Activity Tracker to monitor for abnormal activity and comply with regulatory audit requirements. The events that are collected comply with the Cloud Auditing Data Federation (CADF) standard.

The Activity Tracker service enables you to set the activities and events you want to track. The service provides pre-defined Kibana dashboards to monitor and analyze event logs. The Activity Tracker CLI makes it possible to download all log data to a local or change the retention period.

PaaS and IaaS Sections below provide more information on logging categories and tools available on IBM Cloud platform.

IBM Cloud Organization has strict plans and roadmap to maintain security certifications that we have obtained to ensure and demonstrated the compliance of our cloud platform with the most essential data privacy and security standards.

PaaS Response:

IBM PaaS logging capabilities are integrated in the platform and collection of data is automatically enabled for cloud resources. IBM Cloud, by default, collects, and displays logs for client apps, apps runtimes, and compute runtimes where those apps run.

The State can use the logging capabilities in PaaS to understand the behavior of the cloud platform and the resources that are running in it. No special instrumentation is required to collect the standard out and the standard err logs. For example, you can use logs to provide an audit trail for an application, detect problems in your service, identify vulnerabilities, troubleshoot your app deployments and runtime behavior, detect problems in the infrastructure where your app is running, trace your app across components in the cloud platform, and detect patterns that the State can use to preempt actions that could affect your service SLA.

Logging for Cloud Foundry apps

PaaS records log data that is generated by the Cloud Foundry platform and by Cloud Foundry applications. In the logs, the State can view the errors, warnings, and informational messages that are produced for your app. For more information about logging in Cloud Foundry.

Logging for containers

IBM Cloud records log data that is generated by the IBM PaaS Container Service

Log analysis in PaaS

In PaaS, the State can view the recent logs for your app or tail logs in real time.

Clients can view, filter, and analyze logs through the UI. For more information, see Analyzing logs from the PaaS console.

Clients can also view, filter, and analyze logs by using the command line to manage logs programmatically. For more information, see Analyzing logs from the CLI.

Advanced log analysis with Kibana

In PaaS, clients can use Kibana, an open source analytics and visualization platform, to monitor, search, analyze, and visualize your data in a variety of graphs, for example charts and tables.

Security Logs

Security logs for critical operations in the IBM PaaS Platform are logged to the IBM QRadar SIEM. Tampering of logging configuration and security logs are logged themselves and such logs are delivered to PaaS QRadar. IBM personnel managing PaaS Platform QRadar are distinct from those having privileged access to PaaS Platform and this is enforced using PaaS Platform access governance tool.

Security logs for successful and failed login attempts and critical operations in the IBM PaaS Platform, including network devices, host machines and IDS logs, are logged to IBM QRadar SIEM. IBM QRadar SIEM is configured with a set of rules which trigger offenses based on incoming events across log sources. Those offenses trigger pager duty alerts to the IBM PaaS SOC team on a 24x7 basis.

SaaS Response:

Same as IaaS and PaaS in addition to the following:

Per our Corporate Standard, all IBM SaaS applications monitoring / logging must meet or exceed the controls defined ISO27001 Annex A 12.4. Independent ISO Certification assures the IBM has implemented the following relevant Controls:

- Event Logging: Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed.
- Protection of log information: Logging facilities and log information shall be protected against tampering and unauthorized access.
- Administrator and operator logs: System administrator and system operator activities shall be logged.
- Clock synchronization: The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

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

IaaS Response:

Yes, IBM Cloud can restrict visibility of cloud hosted data to specific users and groups via administrator controlled, policy driven controls. IBM Cloud IaaS identifies and maintains requirements for access within the Logical Access Management Policy, which is based on least privilege and best practices and the Physical and Environmental Protection Policy.

IBM Cloud IaaS's Data Security Architecture is designed using industry standards and best practices, NIST 800-53. We can logically segment client data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's

data. IBM Cloud IaaS employs logical segmentation in all networks and the hypervisors enforce compute isolation in Virtual Machines.

While IBM provides computing resources, technologies, and services on IBM IaaS cloud platform it is the State's responsibility to define and implement features that restrict visibility of cloud-hosted data and documents to specific users or groups.

As a user of an IBM Cloud account, the State can appoint your own administrators to manage your IaaS organizations, spaces, and user roles using the IBM Cloud Administrative tool. Using that tool, you can define your own policies to limit a user's access to specific data and features.

As part of the IaaS Cloud offering, IBM does not own and manage your data, therefore, IBM is not responsible for implementing data entitlement features, but, we can provide for such features as part of the data management services that can be agreed upon between you and IBM, as part of a separate DOU for IBM Cloud services.

PaaS Response:

PaaS access can be defined through the User Access Management tool. The State can appoint your own administrators to manage your PaaS organizations, spaces, and user roles as described in PaaS documentation.

SaaS Response:

As described in Question 8.6.5, any IBM access to customer's SaaS application data or documents is solely for the purpose of providing Administrative or Operational job function. We limit this access to least required access privilege. Per our Corporate Standard, all IBM SaaS applications access control must meet or exceed the controls defined ISO27001 Annex A.9. Independent ISO Certification assures the IBM has implemented the following relevant Controls:

Business Requirement for Access Control.

- Access Control Policy – An access control policy shall be established, documented and reviewed based on business and security requirements for access.
- Access to networks and network services- Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

User Access Management.

- User Registration and deregistration – A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
- User access provisioning - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
- Management of privileged access rights - The allocation and use of privileged access rights shall be restricted and controlled.
- Management of secret authentication information of users - The allocation of secret authentication information shall be controlled through a formal management process.

- Review of User Access Rights – Management shall review user's access rights at regular intervals using a formal process.
- Removal or adjustment of access rights - The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

User Responsibilities.

- Use of secret authentication information - Users shall be required to follow the organization's practices in the use of secret authentication information.
- System and application access control.
- Information access restriction - Access to information and application system functions shall be restricted in accordance with the access control policy.
- Secure log-on procedures - Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
- Password management system - Password management systems shall be interactive and shall ensure quality passwords.
- Use of privileged utility programs - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
- Access control to program source code- Access to program source code shall be restricted.

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.

IaaS Response:

The IBM Cybersecurity Incident Response team (CSIRT) is engaged wherever there is a suspected security incident involving any IaaS, PaaS, SaaS, or your system or data. IBM Cloud Organization has a security incident response plan that aligns with IBM Cybersecurity Incident response

IBM IaaS operations follow IBM CSIRT procedures for any internal breach that impacts the IBM Cloud internal infrastructure and they will notify the State immediately as appropriate following IBM CSIRT internal procedures.

In responding to security incidents on IBM Cloud IaaS platform, IBM Cloud organization follows the relevant ISO 27001 Controls. IBM objective is to notify any affected customers as immediately as physically possible, when and if it is determined that a material breach of their data has occurred. This will be done via direct contact with the customer focal point through agreed-upon channels, and as per the corresponding security controls, as follows:

- Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible.

- Assessment of and decisions on information security events - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

As required, we can accommodate various notification requirements that will meet applicable laws and pending the categorization type of the data being processed or stored on IBM Cloud platform.

PaaS Response:

IBM PaaS has a security incident response plan that aligns with IBM Cybersecurity Incident response process and the IBM Cybersecurity Incident Response team (CSIRT) is engaged wherever there is a suspected security incident involving any PaaS or State system or data. That scope covers any incidents related to privacy.

SaaS Response:

IBM has adopted practices and procedures for internal IBM cyber security incident management by creating CSIRT. CSIRT is managed by the IBM Chief Information Office (CIO) and staffed with CIO and Global Technology Services (GTS) cyber security incident handling and analysis teams. CSIRT's core functions are to provide continuous cyber security incident response and data analysis services, as well as contributing to the ongoing improvement of IBM's overall IT security posture and policies. NIST SP800-61 has informed the development and remains the foundation of CSIRT processes.

The relevant SaaS ISO 27001 Controls implemented and audited writing the IBM CSIRT process are as follows. IBM objectives are always to notify any affected customers as immediately as physically possible, when and if it is determined that a material breach of their data has occurred. This will be done via direct contact with the customer focal point through agreed-upon channels:

- Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible.
- Assessment of and decisions on information security events - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

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.

IaaS Response:

IBM Cloud provides strict security controls, both physical and virtual, to isolate servers and networks hosted on our infrastructure. IBM Cloud architecture enables the ability to provision physically isolated private clouds within the IBM Cloud fabric, not merely virtual private clouds that only rely on 'virtual' isolation from other tenants.

Firewalls, both virtual and physical are primary means to provide for establishing security zones, and to isolate servers, networks and private clouds within our cloud infrastructure. They prevent unwanted traffic from hitting the State's servers, reducing the likelihood of an attack and allowing your server resources to be dedicated for their intended use.

We provide network devices, both physical and virtual, that are used to isolate instances of cloud solutions deployed on the IBM Cloud platform.

As an example, the FortiGate Security Appliance on IBM Cloud deploys an HA-pair of FortiGate Security Appliance (FSA) 300 series devices, and it provides firewall, routing, NAT, and VPN services to protect the public network connection to the State's environment.

FortiGate Virtual Appliance on IBM Cloud service deploys an HA-pair of FortiGate Virtual Appliances that can allow you to reduce risk by implementing critical security controls within your virtual infrastructure.

With IBM Cloud Foundry Enterprise Environment (ICFEE), the State can instantiate multiple, isolated, enterprise-grade Cloud Foundry platforms on demand. Instances of the IBM Cloud Foundry Enterprise service is run within your own account in the IBM Cloud, and can be deployed on either shared or dedicated hardware (Kubernetes clusters).

On shared hardware, virtual isolation gives the State full control over the environment, including capacity changes, change management, services exposed, and user services.

In addition, with hardware isolation, you get single-tenant compute for your environment. IBM Cloud provides the unique capability for you to provision dedicated Bare Metal Servers upon which you can deploy your own VMware-based private cloud. For example, you can enable the creation of a hybrid cloud where on-premises VMware-based servers, tooling, and processes can be extended into the public cloud.

All IBM Cloud IaaS offerings undergo an internal IBM Inter-Enterprise Service (IES) review by a separate dedicated network security team.

PaaS Response:

IBM PaaS network diagrams clearly document the boundaries of different environments and systems including the PaaS data flows across boundaries. IBM PaaS clients are responsible for their own data including compliance with legal standards for that data. The IBM CISO office conducts an annual review of the PaaS network architecture, which includes checks on classification of PaaS data and network zones, and protections between zones.

SaaS Response:

All SaaS applications employ in-depth security defense through multiple physical and logical zones of controls. These layers are manifested in the Infrastructure as described in the IaaS response. All application offerings undergo an internal IBM Inter-Enterprise Service (IES) review by a separate dedicated network security team.

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).

IaaS Response:

IBM Secure Cloud engineering defines comprehensive approaches to secure all components of the IBM Cloud Architecture to satisfy the most stringent infrastructure, application, and data security requirements and policies.

IBM Cloud platform has been architected to enable the best secure engineering practices, and it has layered security controls across network and infrastructure. IBM Cloud provides a group of security services that can be used by application

developers to secure their mobile and web apps. These elements combine to make IBM Cloud a platform with clear choices for secure application development, hosting, and operations.

IBM Cloud Security has been defined to provide for the Six Cloud Security "must have" capabilities, as follows:

- Access management: Identity and access management, privileged identity.
- Network security: Security policy, monitoring, threat protection.
- Data protection: Shadow IT / shadow data, encryption, PII monitoring.
- Application security: Secure application development, vulnerability assessment.
- Visibility and intelligence: Shadow IT / shadow data, monitoring and intelligence, event correlation and alerting, incident response.
- Workload security: Security policy and audit, remediation, patch management.

As part of the Cloud Security implementation, IBM exploits industry-leading products and services to protect our IaaS, PaaS, and SaaS Cloud offerings.

Security and Compliance is the most critical aspect of the IBM Cloud architecture and operations, and its five key components are represented in the figure below as part of the IBM high level layered Cloud architecture.

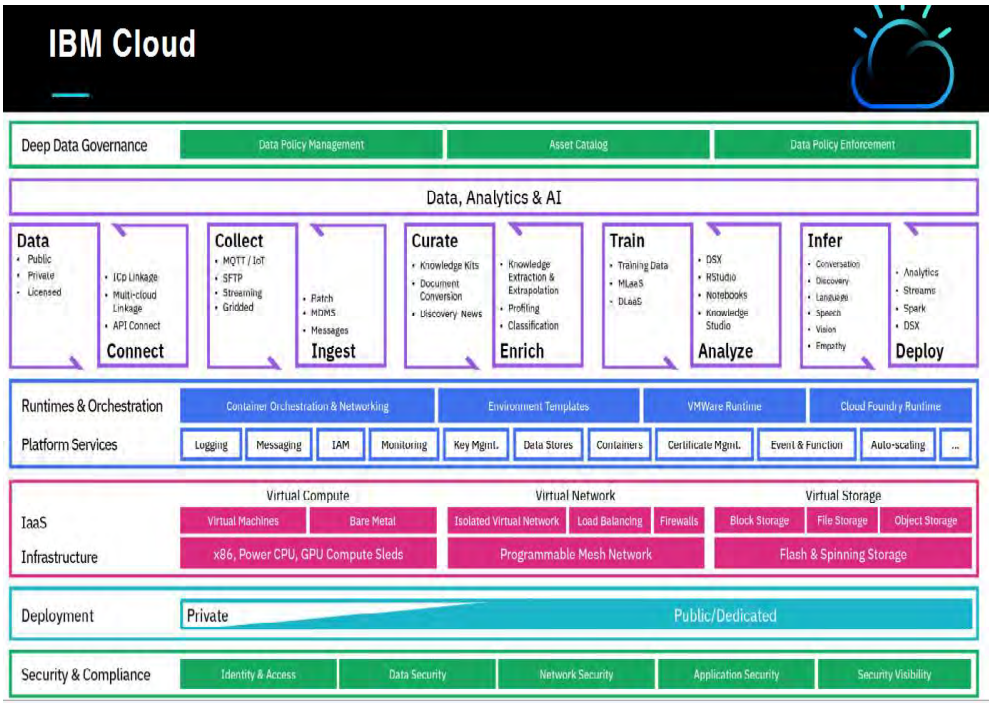

Figure 3: Security and Compliance in the Layered IBM Cloud architecture

The figure below provides a more granular view of the IBM Cloud Public and IBM Cloud Dedicated Platform Security Architecture.

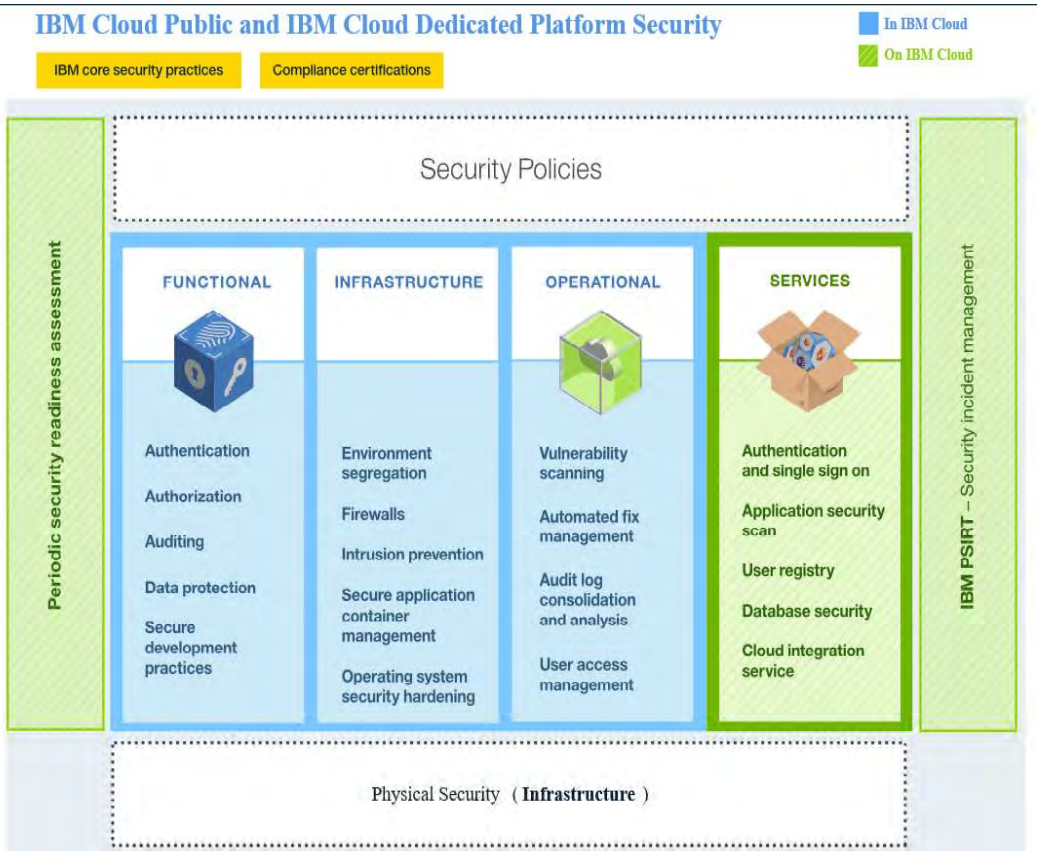

Figure 4: IBM Cloud Security Architecture - Public and IBM Cloud Dedicated Platform

The IBM IaaS Cloud environment is compliant with the most restrictive IBM information technology (IT) security standards, which meet or exceed the industry standards. These standards include the following: Network, data encryption, and access control, as follows:

- Application ACLs, permissions, and penetration testing.
- Identification, authentication, and authorization.
- Information and data protection.
- Service integrity and availability.
- Vulnerability and fix management.
- Denial of service and systematic attacks detection.
- Security incident response.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS response.

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.

IaaS Response:

IBM Corporate HR policies dictate that employment candidates are subject to background verification. IBM Secure Engineering standard mandates security education for team members on an annual basis and that security education involves a formal registration that education is complete.

In addition, IBM employees regularly receive notifications on the importance of cybersecurity, asset registration, and asset security via email, online resources, and others. Privileged laptops are required for access to the State's environments or where the user is a privileged user for a specific regulatory requirement. Owners of those laptops are required to install and maintain full-disk encryption and other increased security controls to satisfy regulatory standards.

As a fundamental principle, no IBM employee has access to your data hosted on IBM IaaS Cloud offering, unless specifically requested by you as part of the DOU for IBM Cloud services.

To protect the assets and clients' data hosted on IBM Cloud, every IBM Cloud data center is fully secured with controls that meet SSAE 16 and other industry-recognized requirements, without exceptions. IBM Cloud is certified for SOC/1/2/3, as well as for NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 31000, PCI-DSS, HIPAA, HITRUST, ITAR and CJIS.

Data and system access and control policy and a formal operational process are outlined in our SOC2 report.

IBM Cloud Activity Tracker tracks how applications and users interact with the IBM Cloud services. State departments can use Activity Tracker to monitor abnormal activity and comply with regulatory audit requirements. The events that are collected comply with the Cloud Auditing Data Federation (CADF) standard. The Activity Tracker service allows you to set the activities and events you want to track. The service provides pre-defined Kibana dashboards to monitor and analyze event logs. The Activity Tracker CLI makes it possible to download log data to a local machine or change the retention period.

PaaS Response:

IBM Corporate HR policies dictate that employment candidates are subject to background verification. IBM PaaS does not use contractors or other third parties to access client environments. IBM Secure Engineering standard mandates security education for team members on an annual basis and that security education involves a formal registration that education is complete. In addition, IBM employees regularly receive notifications on the importance of cybersecurity, asset registration, and asset security via email, online resources, and others. Privileged laptops are required for access to the State's environments or where the user is a privileged user for a specific regulatory requirement. Owners of those laptops are required to install and maintain full-disk encryption and other increased security controls to satisfy regulatory standards.

SaaS Response:

Same as IaaS response.

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.

IaaS Response:

IBM Cloud information security policies and security management approach is aligned with US Government standards and based on the NIST 800-53 framework. This includes the management controls, technical controls, and Operational controls.

With IBM IaaS Cloud offering, securing the customers' data against unauthorized access is a shared responsibility between customers and IBM Cloud Organization. Data that is associated with a running application can be in one of the three following states:

- Data-in-transit: Data that is being transferred between nodes on a network.
- Data-at-rest: Data that is stored in the database, on a file system, or some other type of the data repository.
- Data-in-use: Data that is not currently stored and is being acted upon at an endpoint as part of the transaction execution or some other data processing activities.

Each category of data state needs to be considered when you plan for data security.

The IBM Cloud platform secures data-in-transit by securing the user access to the application by using SSL through the network until the data reaches IBM DataPower Gateway at the boundary of the IBM Cloud internal network. IBM DataPower Gateway, as an example, acts as a reverse proxy and it provides SSL termination. From there to the application, IPSEC is used to secure the data as it travels from the IBM DataPower Gateway to the application.

Security of both data-in-use and data-at-rest is customers' responsibility as they develop and implement their applications. To secure your data, you can take advantage of several technologies and services that available for you in the IBM Cloud Catalog.

There are several technology choices available to secure the data-at-rest. Some technology are database native and others are provided as part of the IBM IaaS platform, for example:

- Encryption for data-at-rest data using AES 256 is currently available in several IBM Cloud data centers, including Dallas, Washington, London, Frankfurt, Amsterdam, Paris, Oslo, Sydney, Melbourne, Toronto, Mexico, and Hong Kong.
- VMware vCenter Server on IBM Cloud provides storage with data encryption at-rest.
- Block and File storage provide data-at-rest data: Disk level with provider managed keys.
- IBM Cloud Backup eVault (Multi-tenant environment) service provides data-in-transit and data-at-rest encryption.

There is abundance information on the data security on IBM Cloud Data Security website (publicly available).

PaaS Response:

All IBM PaaS Platform data is encrypted in-transit. Data-in-transit encryption uses TLS from internet to the reverse proxy at edge of the PaaS network, which terminates TLS. IPSEC-based encryption is provided within the PaaS network for all data in transit from the reverse proxy to PaaS components. IBM PaaS clients must ensure their applications are TLS enabled. Custom certifications can be associated with the PaaS application endpoints using the UI.

Data at rest encryption for a PaaS application's data is the responsibility of the application developer, and they can use services provided by IBM PaaS to do so. See details under the Cloud Data Services section of the PaaS Services catalog.

SaaS Response:

Same as IaaS and PaaS responses combined.

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.

IaaS Response:

For customer managed IaaS environments, the customers are responsible for reporting a data breach to cardholders unless IBM has been engaged to manage the environment. Customers own the data and solution components, and they are responsible for data security and resilience.

As indicated in Section 8.6.8 above in this document, the IBM Cybersecurity Incident Response team (CSIRT) is engaged whenever there is a suspected security incident involving any IaaS, PaaS, SaaS, or your system or data.

IBM IaaS operations follow IBM CSIRT procedures for any internal breach that impacts the IBM Cloud internal infrastructure and they will notify the State immediately as appropriate following IBM CSIRT internal procedures.

In responding to security incidents on IBM Cloud IaaS platform, IBM Cloud organization follows the relevant ISO 27001 Controls. IBM objective is to notify any affected customers as immediately as physically possible, when and if it is determined that a material breach of their data has occurred. This will be done via direct contact with the customer focal point through agreed-upon channels.

In the event of a breach into your system or data, IBM will cooperate with the State to gather information necessary for a notification process and any resulting investigation.

The following is an outline of the process to handle a cybersecurity incident involving IBM managed components (system/data):

- Commercial client identifies a suspected or confirmed cybersecurity incident involving an IBM managed component (system/data).
- Commercial client reviews IBM/client contract for incident reporting guidance.
- Commercial client contacts designated IBM contact per the contract.
- IBM (Account DPE, Employee, and Contractor) is notified by a Commercial client of a potential or confirmed cybersecurity incident.
- If IBM-managed component is not involved, IBM partition ends.

Otherwise,

- IBM (Account DPE, Employee, and Contractor) calls local IBM Help Desk and selects correct VRU choice to report a cybersecurity incident.
- IBM Incident Contact Center (ICC) receives Incident Reporter phone call and activates the IBM CSIRT internal cybersecurity incident process which will immediately trigger activities needed do identify the issue, and to start its mitigation.

The IBM account, operating under the IBM CISRT process and consistent with IBM legal direction, is responsible for meeting contractual requirements for service delivery and for keeping the purpose of audits and communicating with the State regarding the incident. The account team is 100% responsible for reviewing the contract during a cybersecurity investigation and meeting all contractual communication requirements outlined in the State's contract. That includes notifying the proper individuals under the agreed-upon timelines through the approved methods of communication.

In addition, IBM Security offers the IBM X-Force Incident Response and Intelligence Services (IRIS) that team can be engaged directly as part of a Separate DOU. The X-Force IRIS Team has expertise to help you stay ahead of cyber criminals, and it provides services ranging from strategic advisory consulting, incident response, design and deploy services to cloud and managed security services. Our security services enable you to activate global intelligence, innovate without introducing risk, and mature your program over time, as needed to secure a contract for State-owned and managed environments.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS and additional capabilities as described in each SaaS respective Service Description.

8.7 (E) MIGRATION AND REDEPLOYMENT PLAN

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

IaaS Response:

IBM may modify a Cloud Service, without degrading its functionality of security features.

IBM may withdraw a Cloud Service on 12 months' notice, unless otherwise stated in a Transaction Document (TD), IBM will continue to provide the Cloud Service for the reminder of client's unexpired term or work with client to migrate to another IBM offering.

IBM may enable client to continue to use existing instances of a withdrawn service during a transition period.

For those services that are identified as Tier 1 in the IBM Cloud UI, IBM will not withdraw the service without making a functional equivalent available or providing at least five years' notice of the withdrawal.

If IBM disables or modifies an API, IBM will use commercially reasonable efforts to provide 1) advance notice of such change; and 2) continued support for prior versions of the API for a reasonable period of time, unless there are operational, legal, or security risks or burdens.

If IBM Cloud is no longer contractually obligated to maintain the service, we will follow agreed upon with your procedures to either sunset operations of your affected systems, or we will work with you to migrate your systems on new platform, or enable a replacement service offering, if IBM Managed Services are engaged as part of a separate DOU.

Otherwise, since the customers own and operate their systems, applications and databases on IBM Cloud IaaS platform, they are responsible for taking an appropriate action to ensure the continuity of operations, and plan to accommodate for any changes or replacements of a specific offering. IBM Cloud will fully support you in that transition.

During service offering modification or termination, IBM Cloud will follow our best Data Privacy and Security practices to ensure the security of your data, as described above in this document in Sections 8.6.5 and 8.6.12.

PaaS Response:

IBM will provide at least 30 days' notice of its intention to discontinue or replace a generally available service. If an equivalent replacement is not provided for at least 12 months from the date of that announcement, IBM will use commercially reasonable means to continue the operation and support of previously deployed instances of the service.

SaaS Response:

IBM SaaS decommissioning and media destruction controls are driven by the ISO27001 requirements for media labeling, handling, storage, and disposal (Annex A.8 Asset Management. An additional level of confidence can be provided as the data centers proposed for processing of these SaaS applications comply with NIST Controls in this area, and are FedRAMP Compliant.

Physical media received from customers is handled separately from IBM data, but is also inventoried and handled in a controlled manner. Records are kept concerning its lifecycle from being shipped to IBM to its being disposed of, either returned or destroyed.

Media, storage devices, and computing devices being returned to an IBM asset center must be "wiped" to render the data unreadable before shipment.

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.

IaaS Response:

On the IBM Cloud Platform, our customers own their data and are responsible for managing any aspects associated with data ownership.

As per contract terms, IBM Cloud IaaS offers provisions to allow customers to back up their data, or a process to return customer data, prior to secure destruction of that information.

We will remove your data from IBM computing resources following corresponding procedures upon the expiration or cancellation of the cloud service, or earlier upon your request.

IBM may charge for certain activities performed at the Purchasing Entity's request (such as, delivering content in specific format. IBM may assist you in transitioning your content to an alternative technology for an additional charge and under separate terms.

A few of the standard options to return the data back to the customers are as follows:

- Send the requested data using FTP/SFTP, as per preference.
- Return the data on a USB drive provided by the client. IBM will load the data and send it back encrypted.
- Provide the data as part of the IBM Cloud Mass Data Migration service, which uses NAS as part of the solution.

PaaS Response:

Because the State is responsible for data in PaaS, there would be no return of data by IBM unless the State has contracted IBM Managed Services.

SaaS Response:

The specific process for return of customer data differs based on SaaS applications. However, per contract terms, all IBM SaaS applications provide provisions to allow our customers to back up their data, or a process to return customer data, prior to secure destruction of that information.

8.8 (E) SERVICE OR DATA RECOVERY

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

a. Extended downtime.

IaaS Response:

IBM Cloud IaaS platform is designed and implemented to facilitate nearly continuous operations through the infrastructure redundancy, and it provides technologies that allow deploying business continuity and disaster recovery solutions that meet most demanding SLAs and Recovery Time Objectives (RTO).

Since the customers own and manage applications, data, and underlying infrastructure on IBM IaaS platform, they are responsible for defining the business continuity and disaster recovery solutions and plans that will satisfy their operational SLAs.

In circumstances of an extended IBM Cloud IaaS failure, we would switch to a failover data center located at another region where we would restore operations of the infrastructure hosting your applications and databases. That would be done in accordance with the disaster recovery solution designed by you, or IBM

Business Continuity and Resilience Services (BCRS) organization, if engaged as part of a separate DOU.

Infrastructure services downtime is the total accrued minutes a client-identified Infrastructure Service is unavailable due to a service disruption based on an outage type listed in the following table, as measured from the time of a validated outage affecting the identified service until the time such service is available, as validated by IBM support or system records.

For each 30-continuous minute period of downtime, the State will receive a credit in the amount of five percent of the monthly charges for the identified services directly impacted by the outage. Any period during which downtime is less than 30-continuous minutes will not be eligible for credit. Downtime for different services may not be combined to meet this calculation.

Outage Type
Public Network
Private Network
Redundant Infrastructure Power and HVAC

Figure 5: IBM Cloud - Outage Types

If the IBM IaaS Offering experiences a system failure, IBM will use reasonable efforts to minimize downtime when replacing failed hardware and hardware components or performing a scheduled hardware upgrade. IBM will provide the following specified credit:

- For hardware replacement, except as noted below and based on the time to replace, from the time IBM verifies a client-reported hardware failure.
- For planned hardware upgrades, based on the total downtime of the service receiving the upgrade. Service level time periods exclude any time required to reload the operating system or applications or time performance may be degraded. For failure to meet a specified service level time, the State will be eligible for a credit based on the monthly charge for the service affected by the hardware replacement or upgrade, as shown in the following table.

Service Level Time Period	Credit Percent *
≤ 2 hours	none
> 2 hours	20%
> 6 hours	40%
> 10 hours	60%
> 14 hours	80%
> 18 hours	100%

* For POWER8 servers, the service level does not apply; IBM will use commercially reasonable efforts to replace a failed POWER8 server, and there is no credit for failure to meet the above service levels.

Figure 6: IBM Cloud - Customer credits due to SLA meeting failure

Please, refer to the IBM Cloud Service Description document included in the IBM Appendix I IBM Cloud Service Descriptions Example_US, submitted with our response, which defines some of the terms as related to Data Recovery services.

PaaS Response:

PaaS can be deployed with HA and DR in mind. This is achieved by deploying multiple independent PaaS instances within a region and additional instance at least 500 miles away from the main deployment site. Customer application requiring continues availability should be deployed in PaaS with multiple instances and a common load balancer to provide resiliency and improved over-all application performance. In the event of an extended outage, the remaining platform instances can continue to serve customer applications without service interruption. In service interruption, customer is provided with the credits based on the SLA schedule in the IBM Cloud Service Description document included in the IBM Appendix I IBM Cloud Service Descriptions Example_US submitted with our response which defines the terms as related to Data Recovery services.

SaaS Response:

Per ISO27001, all IBM SaaS applications must have the following Controls in place to address extended down time (continuity):

- Information security aspects of business continuity management.
  - Information security continuity.
    - Planning information security continuity: The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
    - Implementing information security continuity: The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
    - Verify, review and evaluate information security continuity: The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
  - Redundancies.
    - Availability of information processing facilities: Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

SLAs govern financial responsibility in the event of an extended downtime. Multiple data centers are employed to deliver services in the event of a disaster.

b. Suffers an unrecoverable loss of data.

IaaS Response:

Since the customers own and manage applications, data, and underlying infrastructure on IBM IaaS platform, they are responsible for defining the business continuity and disaster recovery solutions and plans that will satisfy their operational SLAs.

As indicated in subsection (a) above IBM Cloud IaaS platform is designed and implemented to facilitate continuous operations through infrastructure redundancy, and it provides technologies that allow deploying business continuity and disaster

recover solutions that meet most demanding SLAs and Recovery Time Objectives (RTO).

IBM Cloud provides various types of backup technologies and services that you can engage to back up your servers and data. Our backup and restore service are designed to allow clients to restore files if the primary copy is lost or corrupted. Database backup of DB2, MS SQL, Oracle & Sybase instances is available, and it provides twice weekly full DB backup with 3 times daily incremental (log file) backups.

IBM Cloud Object Storage Services

This solution has a high degree of availability due to the dispersed nature of the solution, but the solution also provides for the capability to mirror data if required by the client.

PaaS Response:

Since the State owns and manages applications and data on IBM PaaS platform, they are responsible for defining the business continuity and disaster recovery solutions and plans that will satisfy their operational SLAs.

SaaS Response:

All IBM SaaS applications backup data on a regular basis. The frequency of these backups may vary depending on the volatility and nature of the data. Some applications maintain and 'active-active' data strategy to minimize data loss. Other applications are backed up in a more traditional approach of daily differential, plus weekly full copy. Customers are also advised to maintain backups should they require additional frequency.

c. Offeror experiences a system failure.

IaaS Response:

In circumstances of an extended IBM Cloud IaaS failure, we would switch operations to a failover data center located at another region where we would restore operations of the infrastructure hosting the State's applications and databases. That would be done in accordance with the disaster recovery solution designed by you, or IBM BCRS organization, if engaged as part of a separate DOU.

IBM Cloud has policies, processes, and procedures defining business continuity and DR in place to minimize the impact of a realized risk event and is properly communicated to tenants. Disaster Recovery and failover of customer data and data processing is the responsibility of the customer.

As part of IaaS offering, for virtual and physical server environments, restore and recovery is a customer responsibility that may be supported by IBM Cloud personnel, as specified by the DOU.

Each IBM Cloud data center has been designed to provide for high level or reliability and resiliency, and they are equipped with backup power, including UPS and Power Generators. Heating and cooling (HVAC) mechanisms are deployed, such as CRAC units, CRAH units, air handlers and/or chillers, to monitor and control temperature and humidity.

Power Distribution Units (PDU) and electrical panels exist in the Premises.

Each IBM Cloud facility is equipped with generators that automatically supply power to the facility in the event of outside power failure. Maintenance contracts are in place to ensure the equipment is maintained to vendors' specifications. The generators are run and tested on a periodic basis under load and no-load conditions and necessary routine maintenance is performed.

The following are examples of handling system failure for selected IBM Cloud offerings:

IBM Cloud Object Storage (ICO) Services

Component failure will happen in an ICO solution but IBM Cloud Object Storage Services has architected the solution to be able to handle this and still allow the customer to be able to read and write data during any component failure, be it an Accesser, Slicestor, or the Manager itself.

PaaS Response:

IBM Cloud has policies, processes, and procedures defining business continuity and DR in place to minimize the impact of a realized risk event and is properly communicated to tenants. Disaster Recovery and failover of customer data and data processing is the responsibility of the State.

SaaS Response:

IBM SaaS application compliance with ISO, NIST, FedRAMP controls, or Business Continuity should provide a level of assurance that our customers will not incur a business failure due to utilization of our SaaS applications. These are described in more detail in question 8.8.1(a). However, there are SLA fees and financial liability amounts specified in our contracts. These fees and amounts vary based on SaaS application.

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

IaaS Response:

IBM provides facilities for the State to recover their data within the 4 hour timeframe. IBM Cloud maintains geographically dispersed instances of its control portal which allows operations to continue in event of failure of the primary site. In addition to data centers containing compute, local storage, among others, IBM Cloud facilities are connected via high speed network capability, backup/restore, and global load balancing which allows clients to quickly and cost effectively achieve disaster recovery and relocation of assets to a data center that is not affected. The IBM Cloud DR and BC plans are outlined in our SOC2 report and are audited annually. DR plans are executed and audited annually.

For many of the IBM Cloud Offerings, the data restore can be accomplished in less than four (4) business hours. For example:

IBM Cloud Object Storage Services

The IBM Cloud Object Storage has a high degree of availability due to the dispersed nature of the solution, but the solution also provides for the capability to mirror data if required by the client. Thus, the four (4) hour RTO can be met with the appropriate storage solution design in place.

PaaS Response:

The State is responsible for all data in PaaS. IBM provides facilities for the State to recover their data.

SaaS Response:

All IBM SaaS applications backup data on a regular basis. The frequency of these backups may vary depending on the volatility and nature of the data. Some applications maintain and 'active-active' data strategy to minimize data loss. Other applications are backed up in a more traditional approach of daily differential plus weekly full copy.

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

IaaS Response:

IBM Cloud IaaS platform is designed and implemented to facilitate almost continuous operations through the infrastructure redundancy, and it provides technologies that allow deploying DR solutions that meet four business hours or less Recovery Time Objectives (RTO).

IBM Cloud does not provide specific DR solutions as part of its IaaS service, but it enables clients to create highly available solutions using their private network connecting all IBM Cloud DCs and PoPs. IBM Cloud private network connects all of our data centers which enables clients to create their own alternate site DR solutions.

- Zerto on IBM Cloud provides a secure, flexible, and scalable disaster recovery solution. These single tenant environments are deployed on IBM Cloud's data centers, provides cloud application recovery in minutes, and achieves a recovery point objective (RPO) of seconds and a recovery time objective (RTO) of minutes.
- Veeam on IBM Cloud provides continuous availability to enterprise clients through our combined and automated backup and recovery solution. It allows for recovery times under 15 minutes.

IBM Cloud Object Storage Services

Due to the architecture of the IBM Cloud Object Storage Services solution we will regularly offer over twelve (12) 9's of availability so we generally have no need to offer RPO or RTO objectives; it is built into the solution.

PaaS Response:

It is expected that customer applications will be deployed into multiple data centers to provide DR and maintain the operational capability. Providing active-active DR mitigates the requirements for RPO/RTO objectives, which are not published at this time. It is IBM's intent to publish these objectives in the future.

SaaS Response:

As described above, IBM SaaS applications are compliance with ISO, NIST, FedRAMP controls for Business Continuity. RPO objectives vary based on the nature and volatility of the application data. Normally, applications are backup up daily, and we can work with our customers to establish a lower RPO.

RTO/RPO objectives vary by application, but IBM utilizes a combination of redundant infrastructure and data centers to ensure that this recovery time is minimized.

Enhanced RTO/RPO (4 hour/2 hour) is available for most SaaS via an add-on part order.

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

a. Method of data backups

IaaS Response:

IBM Cloud IaaS offers several choices to back up and restore applications and data hosted on our platform, to include the following:

1. eVault, which is what we call a “set and forget” type backup. It is agent based and once clients set the schedule you can expect it to perform the backup tasks as directed. Each eVault storage is designed for a single agent (server). Clients can also order multi-site, which allows you to send backups to another targeted data center. eVault can be added during or after the ordering process.
2. Bare metal servers can be architected to create HA using multiple IBM Cloud data centers and replication of the data. In addition, bare metal servers allow clients the flexibility to bring their own backup solutions to meet their requirements.
3. R1, which does a disk-to-disk backup while eVault runs backups at filesystem level. R1 provides high-performance disk-to-disk server backup that reduces backup time frames from hours to minutes. It also provides bare metal restore and disaster recovery. Like .eVault, it also has agents for more granular levels of backup for applications like MSSQL and MYSQL.4. IBM Cloud provides several database options that provide backup services with geo-redundancy, such as Db2 and Cloudant NoSQL.
4. IBM Cloud DBaaS provides daily, weekly, and monthly automated backups.
5. IBM Cloud Db2 performs daily backups with data encryption. Every Db2 instance has local on-disk encryption set up by default. The State does not need to enable it. IBM Db2 encryption uses Advanced Encryption Standard (AES) in Cipher-Block Chaining (CBC) mode with a 256 bits key. Also, database backup images are automatically encrypted. Backup images are encrypted using AES in CBC mode with 256 bit keys.
6. Zerto on IBM Cloud provides a secure, flexible, and scalable disaster recovery solution. These single tenant environments are deployed on IBM Cloud's data centers, provides cloud application recovery in minutes, and achieves a recovery point objective (RPO) of seconds and a recovery time objective (RTO) of minutes.
7. Veeam on IBM Cloud provides continuous availability to enterprise clients through our combined and automated backup and recovery solution. It allows for recovery times under 15 minutes.
8. Clients may bring their own backup solution.

In addition, IBM Cloud Managed Services (CMS) provide various back up, restore, and DR solutions, as described below.

IBM Cloud Object Storage Services

Because we disperse the data across multiple locations and can withstand a site failure there is no need to backup data stored on an IBM Cloud Object Storage Services dsNet.

PaaS Response:

IBM PaaS clients are ultimately responsible for the data integrity of their workload. Cloud Data services provide guidance on how to backup and recover data. Refer to the specific PaaS Data Service within the IBM PaaS online documentation.

Data retention policies and procedures are defined and maintained in accordance to the applicable regulatory and compliance standard. IBM PaaS settings, metadata, and configurations are backed up regularly to prepare for any unplanned outages in the environment. Application Metadata backups are encrypted and stored into IBM IaaS Evault.

As part of the data backup, which includes system metadata and configurations, IBM completes the following tasks:

- Encrypts all backup copies and manages encryption keys.
- Monitors and manages backup activity.
- Provides the encrypted backup files.
- Restores the requested data.
- Manages scheduling conflicts between backup and fix management operations.

SaaS Response:

All IBM SaaS applications backup data on a regular basis. The frequency of these backups may vary depending on the volatility and nature of the data. Some applications maintain and ‘active-active’ data strategy to minimize data loss. Other applications are backed up in a more traditional approach of daily differential plus weekly full copy.

Backups media created as a result of this process is handled using IBM Controls for Asset Management, including:

Only approved carriers are used to transfer electronic media that may contain unencrypted data. Server media used for backup, records retention, or DR is required to be physically protected against unauthorized use, theft, and damage.

Server storage Media Custodian Handling Customer Data are responsible for accurate media inventory and for reporting any discrepancies according to and using IBM’s SIHP. In keeping with the separation of duties security principle, at least one person not involved in the media operation must perform the inventory (the Storage Media Custodian may participate, but is not permitted to be solely responsible for performing the inventory).

b. Method of server image backups

IaaS Response:

The following are the image backup solutions provided on IBM Cloud:

- IBM Cloud Backup eVault.
- IBM Cloud Back up R1Soft.
- Veeam, which is an optional offering is part of the VMware cloud infrastructure.

Customer can utilize IBM Cloud storage and backup service offerings to restore files or images. If it is standard Backup Services (self-managed), it is up to the client to do so. If it is an IBM Cloud Managed Backup offering, the client would have to place a request by opening a ticket.

IBM Cloud Object Storage Services

We are simply the storage platform for any server backups; this is not a natural function of what IBM Cloud Object Storage Services does.

PaaS Response:

As servers are part of IaaS, please see IaaS response.

SaaS Response:

All IBM SaaS applications work in conjunction with the Infrastructure team to ensure that frequency of backups of system images and other required operational files is sufficient to recover in the event of transient errors, corruption, or hardware failures. The actual backup mechanism is dependent on data center operations for our FedRAMP Compliant data centers.

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

IaaS Response:

IBM Cloud does not access client data. The client may explicitly define and control where data should reside as well as construct handling procedures that meet its policy. IBM Cloud provides the technology and facilities to implement your design and corresponding policies.

The client will select which data centers the compute and storage resources are to be deployed. IBM Cloud does not replicate, move data, and compute, but it provides an infrastructure for the customer to perform those operations that are accomplished fully under a customer‘s control. When deciding which region is best for you to store the data, or deploy computing resources, you need to consider several factors based on your application specific requirements to select the most optimal location.

PaaS Response:

IBM PaaS clients are ultimately responsible for the data integrity of their workload. Cloud Data services provide guidance on how to backup and recover data. Refer to the specific PaaS Data Service within the IBM PaaS online documentation.

Data retention policies and procedures are defined and maintained in accordance to the applicable regulatory and compliance standard. Application Metadata backups are encrypted and stored into IBM IaaS Evault.

SOC2 compliance demonstrates the controls IBM PaaS has in place for data retention of PaaS metadata and logs and to safeguard against the unauthorized access, destruction, loss, or alteration of data stored in IBM PaaS.

SaaS Response:

Backup methodologies vary depending on the SaaS application. Many use a disk to disk methodology using distinct production and non-production sites. Others use traditional tape backup. Only approved carriers are used to transfer electronic media that may contain unencrypted data. Server media used for backup, records retention, or DR is required to be physically protected against unauthorized use, theft, and damage.

Server storage Media Custodian handling Customer Data are responsible for accurate media inventory and for reporting any discrepancies according to and using IBM's SIHP. In keeping with the separation of duties security principle, at least one person not involved in the media operation must perform the inventory (the Storage Media Custodian may participate, but is not permitted to be solely responsible for performing the inventory).

Physical media received from customers is handled separately from IBM data, but is also inventoried and handled in a controlled manner. Records are kept concerning its lifecycle from being shipped to IBM to its being disposed of, either returned or destroyed.

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

IaaS Response:

IBM Cloud includes data centers and points of presence located throughout North America, as represented in the Figure below. That offers our clients flexibility in selecting specific data center locations, as well as it enables options for implementing back up and disaster recovery solutions.

Each IBM Cloud data center features one or more pods, supporting up to 5,000 servers. Space, power, network, personnel, and internal infrastructure are optimized across all locations for continuity of operations.

As an example, some of the IBM Cloud data centers are in Washington, Dallas, Houston, Denver, Seattle, San Jose, Chicago, and Miami.

Figure 7: IBM Cloud - North America Data Centers

IBM Cloud maintains geographically dispersed instances of its control portal which allows operations to continue in event of failure of the primary site. In addition to Data centers containing compute, local storage, etc., IBM Cloud facilities are connected via high speed network capability, backup/restore, and global load balancing which allow clients to quickly and cost effectively achieve disaster recovery and relocation of assets to a data center that is not affected. The IBM Cloud DR and BC plans are outlined in our SOC2 report and are audited annually. DR plans are executed and audited annually.

Cloud Managed Services (CMS) data centers in US are located at Raleigh and Boulder with potential for additional sites. CMS sites are interconnected to 23 IBM Cloud data centers worldwide and they offer data backups using IBM Cloud Interconnect services.

PaaS Response:

See IaaS response.

SaaS Response:

Same as IaaS.

IBM's FedRAMP Compliant Data Centers located in Washington DC and Dallas are specifically located based on DR Strategy. IBM SaaS DR Processes are governed by the following ISO 27001 Controls.

- Organization of information security (7 controls).
- Operations security (14 controls).
- Information security incident management (7 controls).
- Information security aspects of business continuity management (4 controls).

8.9 (E) DATA PROTECTION

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

IaaS Response:

With IBM Cloud, securing the State's data against unauthorized access is a joint effort between IBM Cloud and you. Data that is associated with a running application can be in one of three states:

- Data-in-transit: Data that is being transferred between nodes on a network.
- Data-at-rest: Data that is stored in the database, on a file system, or somewhere else.
- Data-in-use: Data that is not currently stored, and is being acted upon at an endpoint.

Each type of data needs to be considered when you plan for data security.

Security for both data-in-use and data-at-rest is the State's responsibility as you develop your application. The State can take advantage of several data-related services available in the IBM Cloud Catalog to help with these concerns.

There are several technology choices available to secure the data-at-rest, and some include database native technology, or they are provided as part of the IBM IaaS platform, for example:

- Encryption for data-at-rest using AES 256 is currently available in several IBM Cloud data centers, to include Dallas, Washington, London, Frankfurt Amsterdam Paris, Oslo, Sydney, Melbourne, Toronto, Mexico, and Hong Kong.
- VMware vCenter Server and VMware Cloud Foundation on IBM Cloud provides vSAN storage with data encryption at rest.
- Block and File storage provide data-at-rest encryption: Disk level with provider-managed keys.
- IBM Cloud Backup eVault (Multi-tenant environment) service provides data-in-transit and data-at-rest encryption.

More information on the data encryption can be found in Section 8.5.1 above in this document.

PaaS Response:

All IBM PaaS Platform data is encrypted in transit. Data-in-transit encryption uses TLS from internet to the reverse proxy at edge of PaaS network, which terminates TLS. IPSEC-based encryption is provided within the PaaS network for all data-in-transit from the reverse proxy to PaaS components. IBM PaaS clients must make sure their applications are TLS enabled. Custom certifications can be associated with the PaaS application endpoints using the UI.

Data-at-rest encryption for a PaaS application's data is the responsibility of the application developer, and they can use services provided by PaaS to do so. Please see details under the Cloud Data Services section of the services catalog.

SaaS Response:

Data encryption at-rest, processing, and in-transit is part of the mandatory requirements in the IBM Secure Development Framework for all of our SaaS applications. All applications either meet this requirement, or are in the remediation process at the current time. Our FedRAMP compliant data centers support encryption in-transit via TLS and PKCS. Cryptography Controls are covered under each SaaS application adherence to the following ISO 27001 Annex A 10 Controls:

- Cryptographic controls.
- Policy on the use of cryptographic controls: A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
- Key management: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

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.

IaaS Response:

IBM can execute a BAA with the State or Purchasing Entity.

PaaS Response:

IBM can execute a BAA with the State or Purchasing Entity.

SaaS Response:

IBM SaaS has a standard BAA that we can use for the specific SaaS apps that are HIPAA ready. We can discuss which applications are ready for HIPAA.

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

IaaS Response:

On the IBM Cloud IaaS platform, at no time will IBM have access to or mine or use the State's data for any purpose. To the extent that managed or professional services are contracted for that involve handling your data, IBM will strictly adhere to the scope of the managed services contract. Under no circumstances IBM Cloud would resell or redistribute information or data that are owned by our customers on our IBM Cloud IaaS platform.

Please, refer to the PaaS and SaaS Responses below for more information on IBM Cloud polices handling customers' data.

PaaS Response:

IBM has no access to the State's data. IBM can copy server image but has no access to your data. The State is responsible to assure data security for its workloads. IBM Managed Services can be engaged to offer backup and disaster recovery services.

SaaS Response:

IBM has no access to the State's data.

IBM's data security policies for SaaS services are published in the Data Security and Privacy Principles, included with our submission as IBM Appendix VIII Data Security and Privacy Principles - Z126-7745-WW-3_05-2018_en_US.pdf, which is incorporated by reference into the applicable Service Description or SOW. Why IBM may change the data security policies from time to time and such changes will also be incorporated by reference provided that such changes will not materially degrade the security of the Cloud Service.

The specific security features and functions for each Cloud Service are described in its Service Description.

IBM will comply with its obligations under data protection laws and regulations applicable to IBM as a provider the Cloud Service, and will provide assistance reasonably necessary for the client to comply with client's obligations under such laws and regulations to use the Cloud Service.

IBM will exercise oversight of its subcontractors who store or access data on behalf of IBM to commit such subcontractors to meet security, privacy, and regulatory standards substantially similar to those of IBM with respect to the content.

If the Cloud Service as described in the Service Description is marketed and designed to receive information that could result in substantial harm to an individual if compromised or is subject to special regulatory handling requirements, then IBM will provide additional security measures as specified in the Service Description.

IBM states in its Cloud Services Agreement that it will not misappropriate your data for any reason.

8.10 (E) SERVICE LEVEL AGREEMENTS

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

IaaS Response:

The IBM Cloud IaaS Service Level Agreement (SLA) defines standards terms, conditions, and availability of the infrastructure offerings IBM Cloud provides to our clients. The SLAs establishes the best services we can offer; therefore, we typically do not allow any modifications to its content.

The sample Service Level Agreement (IBM Cloud Service Description document) can be found in the IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

As part of an extension, or a separate DOU agreement, we can add services and offerings for the State that can have different SLAs than those described in our standard Service Level agreement, thus accommodating different needs for different workloads or service arrangements.

PaaS Response:

Same as IaaS. Please refer to the IBM Cloud Service Description document included IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

SaaS Response:

Same as IaaS. Please refer to the IBM Cloud Service Description document included IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

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.

IaaS Response:

For a sample IBM Cloud Service Level Agreement, Please refer to the IBM Cloud Service Description document included IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

The IBM Cloud SLA defines Availability SLAs for Platform (PaaS) and Infrastructure Services (IaaS), IBM Cloud Object Storage Offering, and Infrastructure Hardware Replacement and Upgrade. It also covers essential topics, to include Cloud Services Usage, Technical Support, Service Charges, Billing, Ordered Services Renewals, and Services Suspension and Termination.

PaaS Response:

Please refer to the IBM Cloud Service Description document included IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

SaaS Response:

Please refer to the IBM Cloud Service Description document included IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

8.11 (E) DATA DISPOSAL

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

IaaS Response:

IBM will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with NIST guidelines for media sanitation. IBM's data overwrite processes adhere to the NIST Special Publication 800-88 Guidelines for Media Sanitization (NIST SP-800-88).

IBM will return or remove content and data from IBM Computing resources upon the expiration or cancellation of Cloud Services, or earlier upon the State's request. IBM may charge for certain activities performed per your request, such as delivering content in a specific format.

PaaS Response:

IBM PaaS clients are ultimately responsible for the data integrity of their workload. For information on how IBM handles disposal or return of client personal data, please refer to the IBM Appendix VII Data Processing Addendum.pdf which is included with our submission.

SaaS Response:

Data disposal is controlled based on the stringent data lifecycle management procedures described above. From a SaaS perspective, once it is determined that the data must be

destroyed, the process falls to the Infrastructure layer of our FedRAMP Compliant data centers. This ensures DoD level sanitization and/or destruction of media.

8.12 (E) PERFORMANCE MEASURES AND REPORTING

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

IaaS Response:

IBM's comprehensive SLA includes guarantees covering:

- Public Network 100% uptime.
- Private Network 100% uptime.
- Customer Portal 100% uptime.
- Redundant Infrastructure 100% uptime.
- Failed Hardware Replacement within two hours of problem diagnosis.
- Scheduled Hardware Upgrades within two hours of scheduled window.
- The State or IBM Managed Services, if engaged, may configure HA infrastructure for you that will meet as many 'nines' as required to meet your business requirements for the workload; if IaaS is self-managed, the State would be responsible for defining and meeting SLAs for specific workloads.
- IBM offers a wide variety of managed services for which a 99.9% or greater SLA is applicable. These services are available as part of a separate agreement than IaaS.

IaaS Platform Downtime is the total accrued minutes a client-identified Infrastructure Service is unavailable due to a service disruption based on an outage, as measured from the time of a validated outage affecting the identified service until the time such service is available, as validated by IBM support or system records. For each 30-continuous minute period of downtime, the State will receive a credit in the amount of five percent of the charges for the identified services directly impacted by the outage. Any period during which downtime is less than 30-continuous minutes will not be eligible for credit. Downtime for different services may not be combined to meet this calculation.

PaaS Response:

Most IBM PaaS services offer 99.5% SLAs. With IBM Cloud services managed, higher SLAs can be achieved but more restrictions on changes. The current SLAs have been defined in detail in the IBM Cloud Service Description document in IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

SaaS Response:

Many IBM SaaS applications provide SLAs based on multiple levels of uptime. Some SaaS applications provide SLAs with 99.9% uptime. Please refer to the current version of the IBM Cloud Service Description document included as IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission.

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

IaaS Response:

Please refer to Paragraph 8.12.1 above for the uptime service on the IBM Cloud IaaS platform.

The SLAs are defined in detail in the IBM Appendix I IBM Cloud Service Descriptions Example_US included with this submission, and they include the following categories:

- Platform Services.
- Infrastructure Services.
- IBM Cloud Object Storage Offerings.
- Infrastructure Hardware Replacement and Upgrade SLA.

IBM provides SLAs for IBM-branded IBM Cloud Services. Service levels based on downtime do not include time related to exclusions, IBM Cloud UI unavailability or time to reload, configure, enable, or access content or include other services indirectly affected by an outage (Downtime). SLAs are available only if the State is compliant with the Agreement terms and do not apply to any third party including the State's users. SLAs do not apply to beta, experimental, or no-charge Cloud Services.

SLAs are not a warranty and are the State's exclusive remedy for IBM's failure to meet a specified service level. IBM will validate SLA claims based upon information provided and IBM system records. IBM will provide IBM Cloud UI or other notice of approved credits. IBM's reasonable determination of a credit is final. The State agrees to continue to make payment in full for Cloud Services while an SLA claim is being reviewed. Credits may not reduce payments due for a service below zero for any billing period. If an IBM Business Partner sold the State a subscription to the Cloud Service, the monthly charge will be calculated on the then-current list price for the service that causes the SLA claim, discounted by 50%.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM SaaS applications offer different levels of SLAs depending on the nature of their functionality. SLAs can be found in our SaaS Cloud Service Descriptions found in our IBM Appendix VI SaaS Service Description Example - WCA - i126-6994-09_01-2018_en_US.pdf included with our response. The following is an example for Watson Campaign Automation on Cloud.

Availability of the Cloud Service during a contracted month

Availability during a contracted month	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
Less than 99.95%	2%
Less than 99.00%	5%
Less than 98.00%	10%
Less than 97.00%	20%

* If the Cloud Service was acquired from an IBM Business Partner, the monthly subscription fee will be calculated on the then-current list price for the Cloud Service in effect for the contracted month which is the subject of a claim, discounted at a rate of 50%. IBM will make a rebate directly available to Client.

Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month minus the total number of minutes of Downtime in a contracted month divided by the total number of minutes in the contracted month.

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.

IaaS Response:

IBM delivers a world-class client engagement experience that includes how users engage for help, discover answers, and interact with IBM systems, tools, and processes across IBM Cloud. Whether a client is entitled to IaaS, PaaS, SaaS, or Watson platform services, IBM provides a unified support model and a unified part structure that offers Self Service, Basic, Advanced, and Premium Support and provides a "One IBM" client experience.

The Basic, Advanced, and Premium Support provide for 24x7 Support availability with IBM Cloud Support through Tickets, Chat, and Phone.

We provide basic level support at no additional charge for Cloud Services. Advanced support is included as part of a dedicated or private offering and for services executed within those environments. The State can select fee-based technical support offerings that provide additional support benefits. The State may submit a support ticket describing the issue in accordance with the applicable support policy procedures. The support policies for Platform and Infrastructure Services are available in the IBM Cloud UI and provide details of available support options, as well as information on access, support business hours, severity classification, and support resources and limitations. IBM uses commercially reasonable efforts to respond to support requests; however, there is no specified response time objective for basic level support. Unless otherwise agreed in writing, support is available only to you (and your authorized users) and not to users of the State's solutions. The State is solely responsible for providing all client support and services to its users.

The following figure summarizes the IBM Cloud Support Tiered Offerings available in 2018, with some new forms of support being added this year.

Figure 8: IBM Cloud Support Offerings

All IBM Cloud clients can access the free online support in the IBM Cloud UI, also via several other ways, to include our development team and the Cloud community.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS response.

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

IaaS Response:

The IBM Cloud Service Description document included in our IBM Appendix I IBM Cloud Service Descriptions Example_US provided with our submission. It describes how IBM addresses scenarios when we fail to meet SLAs.

PaaS Response:

Please, refer to the IBM Cloud Service Description document in our IBM Appendix I IBM Cloud Service Descriptions Example_US provided with our submission. It describes how IBM addresses scenarios when we fail to meet SLAs.

SaaS Response:

Please refer to the IBM Cloud Service Description document in our IBM IBM Appendix VI aaS Service Description Example - WCA - i126-6994-09_01-2018_en_US.pdf which we've included with our submission. It describes how IBM addresses scenarios when we fail to meet SLAs.

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

IaaS Response:

IBM will maintain and update public instances of the cloud services on a regular basis during scheduled maintenance windows as published in support documentation available in the IBM Cloud UI. IBM will deploy software updates to the State's

dedicated and local environments as scheduled in advance, with appropriate notification to you, with the goal of keeping such environments reasonably current with the public instances.

The IBM Cloud regular maintenance that should not require system downtime ("non-disruptive" maintenance) and maintenance that may require some system downtime and restarting ("disruptive" maintenance") will be performed at the scheduled times published in the IBM Cloud UI that is available to all users of IBM Cloud infrastructure.

PaaS Response:

IBM notifies the State's point of contact for each service when planned scheduled outages occur. If you have a conflict with timing, IBM SRE will work with you on outage time.

SaaS Response:

IBM SaaS applications maintain a scheduled downtime window where changes, updates and other systems maintenance is applied. This window varies by Offering, but is normally scheduled for weekend late evening and/or early morning.

Maintenance schedules are available via standard support portals or the appropriate SaaS Support Handbook for each of the applications.

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

IaaS Response:

The consumers of IBM Cloud IaaS platform offerings are responsible for designing and implementing disaster recovery solutions in alignment with their strategies and expected SLAs using the technologies available on the IBM Cloud IaaS platform.

In case of IBM Cloud IaaS failing to provide the SLA metrics, as associated with the infrastructure needed to operate your DR solution, IBM Cloud will compensate you, as follows:

For each 30 continuous minute period of Downtime, you will receive a credit in the amount of 5% of the monthly charges for the identified services directly impacted by the outage. Any period during which Downtime is less than 30 continuous minutes will not be eligible for credit. Downtime for different services may not be combined to meet this calculation.

Detailed information on the IBM Cloud IaaS SLAs can be found in the IBM Cloud Service Description document included in IBM Appendix I IBM Cloud Service Descriptions Example_US provided with our submission.

PaaS Response:

Please, refer to the IBM Cloud Service Description document in our IBM Appendix I IBM Cloud Service Descriptions Example_US provided with our submission.

SaaS Response:

Please refer to the IBM Cloud Service Description document in our IBM Appendix VI aaS Service Description Example - WCA - i126-6994-09_01-2018_en_US.pdf which is included in our submission.

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.

IaaS Response:

IBM Cloud Application Performance Management (APM) solution allows the State to actively monitor and manage your application infrastructure performance in order to quickly respond and ensure optimal experience for your users. It helps the State monitor and analyze application performance, discover issues, identify root causes, and prevent outages to improve user experience and stability. The reports provided by APM are real time or they include collected data that are used to manage dynamic trends of your application. Some of the key reports provided by the APM solution are:

- Portfolio management.
- Discovery of application components in systems environment.
- Transaction tracking to view application performance.
- Analytics to provide insight and help the State to manage dynamic trends.
- End user transaction performance.

Sample of reports are represented in the figures included below.

Figure 9: IBM Cloud APM - Portfolio Management Report

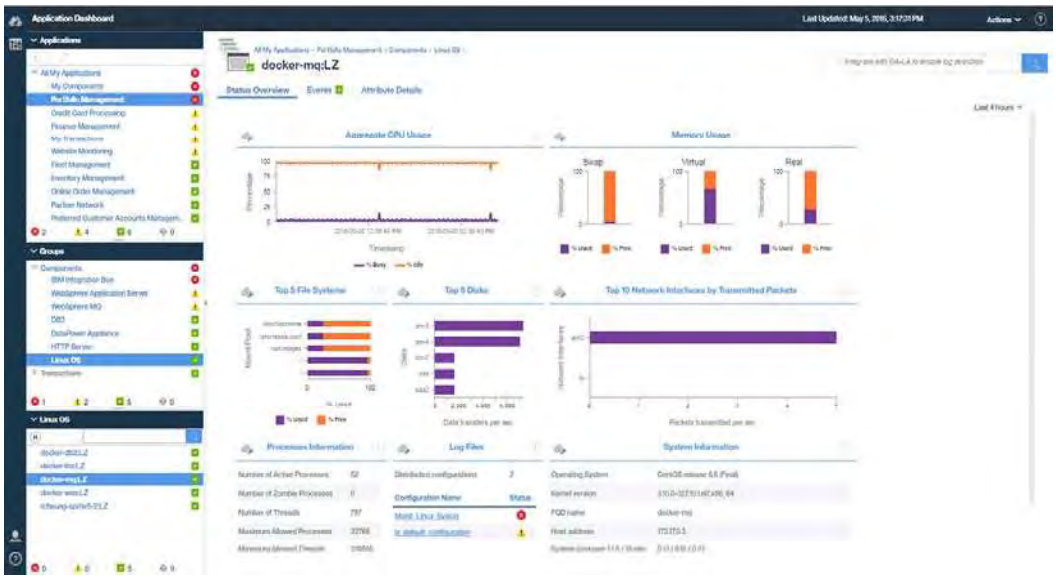

Figure 10: Transaction tracking to view application performance

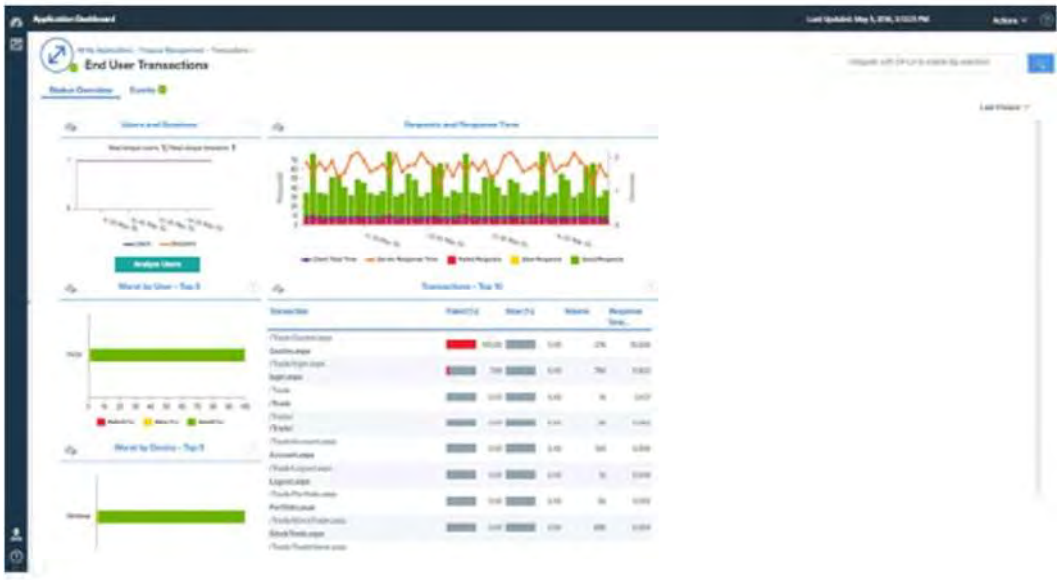

Figure 11: IBM Cloud APM Report - End User Transaction Performance

In addition, IBM Cloud provides application monitoring with New Relic, a software analytics product for APM. It delivers real time and trending data about web application's performance and the level of satisfaction that users experience. With end-to-end transaction tracing and a variety of color-coded charts and reports, New Relic can visualize your data down to the deepest code levels.

Also, the State can use the IBM Cloud Monitoring service to collect, visualize, and retain metrics, and define rules and alerts that notify you of conditions that require attention. Cloud Monitoring can empower your DevOps team with features that give insight into how your apps are performing and consuming resources and allow developers and administrators to quickly identify trends, detect, and diagnose problems; with immediate time to value and low total cost of ownership. Use Visualization by means of Grafana is used to monitor your environment.

The State can also use the IBM Cloud Event Management service to set up real-time incident management for your services, applications, and infrastructure. Cloud Event Management can receive events from various monitoring sources, either on premise or in the cloud. Events indicate that something has happened on an application, service, or another monitored object.

Additionally, IBM Cloud Availability Monitoring helps DevOps teams ensure their applications are always available and meeting user expectations for response time as they roll out continuous updates. The service, which is tightly integrated into the DevOps toolchain, runs synthetic tests from locations around the world, around the clock to proactively detect and fix performance issues before they impact users.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS response

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

IaaS Response:

IBM Cloud provides detailed access to billing and usage through the IBM Cloud API. Billing data can be extracted as .cvs files and programmatically imported into the State's billing system for analysis, verification, and printing.

Reports, such as, Account Summary, Account Usage, Organization Usage, Resource Group Usage, and several others can be also accessed using IBM Cloud APIs.

Detailed information on implementing the usage reports, as well as OpenAPI specifications are available in the IBM Cloud GitHub repository. The IBM Cloud (Cloud) Admin Console provides the ability to view applications and service usage by organizations. A Cloud account has a two-level hierarchy: organizations and spaces. Organizations are divided into spaces and each of these spaces puts a group of services and applications together.

My Billing application provides for the following requirements:

- Users need to check services and applications costs by spaces and not only by organizations.
- They want to export usage information and share it with other teams of their companies.
- They also need to do a quick usage comparison among spaces using a chart and it allows for the following:
  - Monthly usage comparison data is displayed in a single chart.
  - Data can be exported to a CSV or EXCEL file.

In addition, IBM Cloud provides an extensive portfolio of SaaS products that give the ability to generate reports including historical, statistical, and usage data locally.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS response.

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

IaaS Response:

Yes, self elf-service IaaS and PaaS deployment is available on-demand 24x365 in every IBM Cloud data center around the world.

In addition, as part of the Premium Support IBM can assign the State a dedicated Account Technical Manager who can assist you as needed to escalate any urgent requests for service.

PaaS Response:

Same as IaaS response.

SaaS Response:

Where on-demand deployment is supported, 24x365 capabilities are provided.

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

IaaS Response:

Auto-scaling is available 24x365 as it is self-service. Auto-scaling service enables the State to automatically increase or decrease the compute capacity of your application. The number of application instances are adjusted dynamically based on the auto-scaling policy you define.

Auto-scaling offers the following two features:

- Dynamic scaling: Automatically add or remove resources to match the current workload.
- Metric statistics: Visualize the current and historical values of performance metrics.

The control over Auto-Scaling policies is available through the IBM Cloud API, which allows run-time environments to scale up or down based on real-time workload performance and user-configured thresholds. The IBM Cloud provides versatile Auto-Scaling policies based on time, network throughput, CPU, and memory consumption. In contrast, many other Cloud Service Providers provide auto-scaling primary of CPU resources.

PaaS Response:

Same as IaaS response.

SaaS Response:

We have the capability to scale up or down in an elastic fashion, subject to the terms in the Service Description.

8.13 (E) CLOUD SECURITY ALLIANCE

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

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

IaaS Response:

Yes, our CSA STAR Self-Assessment questionnaires for IBM Cloud Infrastructure IBM Cloud Platform and IBM Watson Services have been included in IBM Appendix II Attachment B IBM-Cloud-infrastructure_CAIQ-v3.0.1-April-2018 included with our submission. They are also available on the IBM Cloud information pages.

PaaS Response:

Our CSA STAR Self-Assessment has been provided, please see IBM Appendix III Attachment B IBM-Cloud-platform_CAIQ-v3.0.1-Oct-2017 which has been included in our submission.

SaaS Response:

IBM has chosen the globally recognized, and NIST aligned, ISO27001 Standard as the common set of controls for third party Security ISMS Certification.

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

IaaS Response:

Please see IBM Appendix II Attachment B IBM-Cloud-infrastructure_CAIQ-v3.0.1-April-2018 included with our submission. IBM Cloud's IaaS information security policies and security management approach is aligned with US Government standards and based on the NIST 800-53 framework. This includes the management controls, technical controls, and Operational controls.

PaaS Response:

Please see IBM Appendix III Attachment B IBM-Cloud-platform_CAIQ-v3.0.1-Oct-2017 which has been included in our submission.

SaaS Response:

IBM has chosen the globally recognized, and NIST aligned, ISO27001 Standard as the common set of controls for third party Security ISMS Certification.

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

IaaS Response:

IBM has not completed a CSA STAR attestation, certification or assessment.

PaaS Response:

IBM has not completed a CSA STAR attestation, certification or assessment.

SaaS Response:

IBM has not completed a CSA STAR attestation, certification, or assessment.

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

IaaS Response:

IBM Cloud does not have/follow CSA STAR Continuous Monitoring

PaaS Response:

IBM Cloud does not have/follow CSA STAR Continuous Monitoring.

SaaS Response:

IBM Cloud does not have/follow CSA STAR Continuous Monitoring.

8.14 (E) SERVICE PROVISIONING

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

IaaS Response:

Emergency or rush services implementation are available as part of the Advanced and Premium Support that the Purchasing Entity can purchase from IBM. Both Advanced and Premium Support include an escalation process that will address your requests to accelerate some of the critical or emergency tasks. In addition, Premium Support includes a Technical Account Manager (TAM) who will be dedicated to managing your escalation requests.

PaaS Response:

Processes to provision infrastructure and services are fully automated with self-service and can be requested by the Purchasing Entity via UI or APIs. If the State would like assistance with implementation, you can contract IBM Managed Services

SaaS Response:

Many SaaS provisioning requests, for example new users can be carried out autonomously by our customers. Most existing clients can provision in an elastic fashion. Where there is a requirement for a new instance requiring IBM operational resources, the local IBM client and cloud sales team will work with our customers to execute that request as rapidly as possible.

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

IaaS Response:

The provisioning time for our IaaS solution depends on a specific offering. For the Standard and Public offerings, the provisioning process is an automated self-service. It takes between minutes to a few hours to make the given offering available to the State in our cloud environment.

For example:

- IBM Cloud Virtual Servers can be available to the State in a matter of minutes. The virtual servers are deployed from your choice of virtual server images and in the geographic region that makes sense for your workloads.
- IBM Cloud Bare Metal Servers can be provisioned on demand in IBM Cloud data centers around the world in two to four hours. If the State needs to be online in minutes or only need limited resources, select an hourly bare metal server.

Some of the bare metal server’s features include the following:

- GPUs – servers with cutting-edge GPUs to handle your most complex compute-intensive workloads. NVIDIA Tesla GPUs on IBM Cloud are designed for high performance acceleration of scientific computation, data analytics, and professional-grade virtualized graphics.
- SAP HANA 4-socket and 8-socket bare metal servers are SAP certified for production S/4 HANA workloads, powered by Intel Xeon E7-8890 v4 processors, with up to 8TB of RAM.
- IBM Cloud Storage

  Block Storage: There are two types of Block Storage, Endurance, and Performance. The Purchasing Entity can order the Block Storage from the IBM Cloud infrastructure client portal. New storage allocation should be available in a few minutes for the Standard Public Storage offerings. The time to provision Private Cloud and Custom storage configurations may vary pending specific configuration requirements.
- File Storage: The Purchasing Entity can order File Storage from the from the IBM Cloud infrastructure client portal. Your new storage allocation should be available in a few minutes.
- Object Storage: Before ordering a new IBM Cloud Object Storage instance, it is necessary to create a client account first. After creating a client account, you can immediately order a new object storage service instance by accessing https://console.Cloud.net/, and selecting the Cloud Object Storage tile in the storage section in the IBM Cloud Catalog. After clicking “Create New Storage” instance, you will be automatically redirected to your new instance. IBM Cloud Offering Catalog available on the IBM Cloud website provides an extensive information on provisioning various IaaS Services.

PaaS Response:

The provisioning time for our PaaS solution depends on a specific offering. For the Standard and Public Offerings, the provisioning process is an automated self-service. It takes between minutes to a few hours to make the offering available for you in our cloud environment.

SaaS Response:

The lead time for provisioning IBM SaaS applications varies. This can range from hours for simple, multi-tenant applications, to weeks for complex applications.

8.15 (E) BACK UP AND DISASTER PLAN

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

IaaS Response:

IBM Cloud provides computing and storage resources as needed to meet the most demanding retention periods mandated by the State and your policies or legal requirements. IBM Cloud Certification to ISO27001 requires adherence to the following controls that are concerned with legal retention periods and disposition.

In addition to the technology we offer as part of IBM Cloud platform, our commitment and ability to meeting legal retention periods and disposition is demonstrated through Industry Standards certifications for our cloud platform.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM SaaS Certification to ISO27001 requires adherence to the following Controls:

- Legal retention periods and disposition.
- Compliance with legal and contractual requirements.
- Identification of applicable legislation and contractual requirements - All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
- Intellectual Property Rights (IPR): Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
- Protection of records: Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.
- Privacy and protection of personally identifiable information: Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
- Regulation of cryptographic controls: Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

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

IaaS Response:

IBM Cloud architecture and implementation provides a foundation suited to face the most challenging disaster scenarios.

While the chance is minimal that the IBM Cloud Data Center could be impaired due to disaster events outside of our control, we take that as a high priority operational issue that has to be considered in risk planning and prevention.

Today's disasters come in many varieties, from naturally occurring events (such as hurricanes, earthquakes and floods) to man-made threats, like employee sabotage, hacking and data theft. The list below includes some of the most common disruptive events that should be considered in the disaster risk planning and mitigation:

- Act of war and terrorist attacks.
- Transport shut-downs due to weather and other conditions.
- Earthquakes.

- Weather abnormalities, such as hurricanes and tornados.
- Floods and fires.
- Epidemic illness impacting staffing and operations.
- Massive hardware or software failure.

In circumstances of a disaster scenario that would impact one or more IBM Cloud data centers, we would failover our system operations to another IBM Cloud Data Center located in the US. We would then execute the recovery operations of the infrastructure hosting our customers' systems, as per the procedures specified in the Disaster Recovery Plans, and as needed to meet your Recovery Time Objectives.

PaaS Response:

Same as IaaS response.

SaaS Response:

There are a wide variety of scenarios possible in our portfolio of 150 over SaaS applications which is why IBM requires ISO 27001 Certification of each. This Certification specifically addresses evaluation of failure modes and recovery procedures for all possible scenarios.

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.

IaaS Response:

IBM Cloud includes nearly 60 data centers worldwide in six (6) regions and 18 availability zones. Our availability zone design provides an easier and more effective way to design and operate applications and databases, making them highly available, fault tolerant and scalable.

Within United States, as represented in the figure below, IBM Cloud data centers are located in Washington, Dallas, Houston, Denver, Seattle, San Jose, Chicago, and Miami. This offers our clients flexibility in selecting specific data center locations, as well as it enables options for implementing back up and disaster recovery solutions. Each IBM Cloud data center features one or more pods, supporting up to 5,000 servers. Space, power, network, personnel, and internal infrastructure are optimized across all locations for continuity of operations.

Figure 12: IBM Cloud - North America Data Centers

IBM Cloud maintains geographically dispersed instances of its control portal which allows operations to continue in event of failure of the primary site. In addition to Data centers containing compute, local storage, etc.

IBM Cloud facilities are connected via high speed network capability, backup/restore and global load balancing which allow clients to quickly and cost effectively achieve disaster recovery and relocation of assets to a data center that is not affected. The IBM Cloud DR and BC plans are outlined in our SOC2 report and are audited annually. DR plans are executed and audited annually.

We also have FedRAMP Compliant Data Centers located in Washington DC and Dallas. These are specifically located based on DR Strategy and needs.

There are no interdependencies between IBM Cloud data centers. Network connections between data centers are via private, redundant, and diverse-path high-speed fiber. Each data center has multiple redundant utility connections and each data center is made up of multiple “pods” with no interdependencies between pods. The data centers have redundant N+1 diesel power generation with four days on site fuel storage; perpetual refueling provisions with multiple suppliers are in place.

All power generation plants are tested monthly. Each data center has redundant N+1 cooling, redundant N+1 UPS and redundant PDU’s. The State will have a variety of options to configure self-managed infrastructure to run large-scale applications that run independently and are highly available in disparate data centers. You will also have IBM managed options for critical infrastructure, which IBM will provision and manage steady state to the agreed-upon SLAs.

The IBM Cloud platform provides a number of options to allow clients to deploy applications for high availability including high availability zones within a region and high availability across regions. There are a number of tutorials available at IBM developerWorks and IBM services available to assist the State with the configurations.

PaaS Response:

Same as IaaS response.

SaaS Response:

Same as IaaS.

IBM's FedRAMP Compliant Data Centers located in Washington DC and Dallas are specifically located based on DR Strategy. IBM SaaS DR Processes are governed by the following ISO 27001 Controls:

- Organization of information security (7 controls).
- Operations security (14 controls).
- Information security incident management (7 controls).
- Information security aspects of business continuity management (4 controls).

8.16 (E) HOSTING AND PROVISIONING

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

IaaS Response:

All resources in IBM Cloud are provisioned with standard tags. Standard tags enable client administrators to see where all devices are physically located, down to the individual rack within a POD within a data center.

Please refer to the IBM Cloud Infrastructure API page for detailed information on provisioning processes and managing your infrastructure through APIs.

Bare Metal Servers are the basis for client IaaS solution, and they are dedicated to you and not shared in any part, including server resources, with other clients. These servers are managed by you, are provisioned without a hypervisor, and can be deployed in one or more data centers.

IBM Cloud Virtual Servers are scalable virtual servers that are purchased with dedicated cores and memory allocations. They are fully customized and the State can build-to-suit any virtual server with a number of options. There are no pre-defined package requirements, so you can tune each server to the workload it supports. Virtual servers are provisioned in as few as five minutes, giving you minimal wait time between order and provisioning.

PaaS Response:

The State can choose to provision services from the IBM Cloud catalog or use the IBM Cloud command line. Select the space, organization, region, and service plan and then deploy the service.

SaaS Response:

For IBM SaaS applications, this is dependent on the applications; the details can be found in the relevant IBM SaaS Cloud Services Description. An example can be found in IBM Appendix VI aaS Service Description Example - WCA - i126-6994-09_01-2018_en_US.pdf which has been include in our submission.

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.)

IaaS Response:

IBM Cloud offers several options to deploy new servers, as per configuration required, to include the following:

- IBM Cloud Portal.
- VMWare vCenter.
- VMWare vRealize.
- IBM Cloud Managed Services (CMS) – for custom infrastructure build.
- IBM Cloud Brokerage Solution.

IBM Virtual Servers can be deployed in a matter of minutes from virtual server images of your choice in the geographic region that makes sense for your workloads.

- Public Virtual Servers offer flavors of vCPU and Memory up to 56 cores and 242 GB RAM.
- Dedicated Virtual Servers offer customizable vCPU & Memory up to 56 cores and 242 GB RAM.

IBM Cloud Foundation Offering

When you order VMware Cloud Foundation on IBM Cloud, an entire VMware environment is deployed automatically. The base deployment consists of four IBM Cloud Bare Metal Servers with the VMware Cloud Foundation stack preinstalled and configured to provide a unified software-defined data center (SDDC) platform. Cloud Foundation natively integrates VMware vSphere, VMware NSX, VMware Virtual SAN, and is architected based on VMware-validated designs.

Deploying Bare Metal Servers:

There are a number for Bare Metal Servers options available, thus, corresponding server deployment options, as outlined below.

Bare Metal Servers – Popular.

IBM Cloud offers preconfigured servers that meet the needs of most use cases. These servers are considered "fast provision" because your compute options (number of cores, speed, RAM, and number of drives) are preset, and are ready to configure 30 to 40 minutes after provisioning.

Bare Metal Servers – Custom-based

If one of the popular servers doesn't meet your workload needs, you can customize your Bare Metal Servers to meet your needs. Customized servers are provisioned in 2 to 4 hours and offer a greater variety of cores, speeds, RAM, and drives.

Custom POWER8-based servers

IBM Cloud offers you the option to provision an Intel POWER8-based bare metal server. POWER8 servers are built with the POWER8 processor and an OpenPower-based platform, which is tuned specifically for cloud-based deployments for data, cognitive, and web workloads on Linux.

SAP-certified bare metal servers

IBM Cloud Bare Metal Servers are certified to support your SAP HANA and SAP NetWeaver workloads.

PaaS Response:

Servers are part of IaaS; see above response.

SaaS Response:

SaaS applications, in general, do not require or provide tool sets, as they are fully created applications with browser or app interfaces for configuration, customization, administration, etc. For those Cloud Services which do allow for “extensions”, those extensions can be made in Customer’s preferred development or visual design tool set, including those offered by IBM and third parties.

SoftLayer

New server deployment is accomplished via SoftLayer’s user portal or through our extensive API. Bare metal server deployment, upgrade and provisioning occurs in less than four (4) hours. Virtual servers can be deployed in less than 15 minutes. SoftLayer supports private, hybrid or public clouds. Customers are capable of building their own Hypervisor clusters on bare metal, if desired.

2. Creating and storing server images for future multiple deployments

IaaS Response:

IBM Cloud IaaS infrastructure allows customers to manage backup/restore using our storage offerings. So you can use your own backup tool applied to your IBM Cloud resources. You can leverage our private global network and iSCSI Replication to have your backup located in another data center.

IBM Cloud supports bare metal or virtual image repositories for quick deployment of additional workload either manually or automatically via Auto-Scaling.

- With IBM Cloud Virtual Servers image templates, clients can capture a device's image to quickly replicate its configuration with minimal changes in the order process.
- Standard image templates provide an imaging option for all Virtual Servers, regardless of operating system.
- Standard image templates allow clients to capture an image of an existing virtual server and create a new one based on the captured image. Standard image templates are not compatible with bare metal servers.
- The State will be able to set up your own Docker image repository in a multi-tenant, highly available, and scalable private image registry that is hosted

and managed by IBM. By using the registry, you can build, securely store, and share Docker images across cluster users.

- The image import/export feature that is located on the Image Templates page in the IBM Cloud infrastructure client portal allows for the conversion of VHDs and ISOs stored on an Object Storage account to be converted into image templates and vice versa.
- The Image Templates screen in the IBM Cloud infrastructure client portal allows users to upload an existing image from a Swift-based Object Storage account.
- Only servers that are provisioned by IBM Cloud can be captured and deployed. Individual virtual servers that the State manually created on personal devices cannot be captured, provisioned, or deployed.
- The Image Templates screen in the IBM Cloud infrastructure client portal allows users to upload an existing image from a Swift-based Object Storage account.

To store server images for future deployment, you can use any of the backup solutions provided on IBM Cloud to include the following:

- IBM Cloud Backup eVault.
- IBM Cloud Back up R1Soft Veeam, which is an optional offering is part of the VMware cloud infrastructure.

PaaS Response:

Servers are part of IaaS; see above response.

SaaS Response:

N/A

3. Securing additional storage space

IaaS Response:

IBM Cloud IaaS Offers the following three primary types of storage space:

- IBM Block Storage.
- IBM Object Storage.
- IBM File Storage.

Customers can provision additional storage space as needed via the customer portal on-demand.

Please, refer to the paragraphs below for an overview of securing the storage space on the IaaS platform.

- IBM Block Storage:

  IBM® Block Storage for IBM Cloud is persistent, high performance iSCSI storage that is provisioned and managed independently of compute instances.

Block Storage LUNs can be provisioned from 20 GB to 12 TB with two options for provisioning:

- Provision endurance tiers featuring pre-defined performance levels and features like snapshots and replication.
- Build a high-powered performance environment with allocated input/output operations per second (IOPS).

Ordering of IBM Block Storage can be done in the IBM Cloud Infrastructure customer portal. After completing a few online steps to describe the required parameters of the storage, it will take a few minutes for your storage to be allocated and ready for usage.

- IBM Cloud File Storage:

  IBM Cloud File Storage for IBM Cloud is persistent, fast, and flexible Network Attached, NFS-based File Storage. In this network-attached storage (NAS) environment, you have total control over your file shares function and performance.

  Ordering of IBM Cloud File Storage can be done in the IBM Cloud Infrastructure customer portal. After completing a few online steps to describe the required parameters of the storage, it will take a few minutes for your storage to be allocated and ready for usage.

- IBM Cloud Object Storage:

  IBM Cloud Object Storage is available with three types of resiliency: Cross Region, Regional, and Single Data Center.

  Before ordering a new IBM Cloud Object Storage instance, it is necessary to create a customer account first on the bluemix.net website.

  After setting up an account, you can select cloud Object Storage from the Catalog, select the subscription plan, and click Create - as soon as done, you will be redirected to your new storage instance.

PaaS Resonse:

IBM Cloud Object Storage can be provisioned from the IBM Cloud portal, which includes PaaS and IaaS.

SaaS Response:

Additional storage space, where applicable, is ordered via the Customers preferred or normal purchasing mechanism, including direct from IBM, via IBM Digital Marketplace, third-party public digital marketplaces, via IBM business partners, or through an IBM sales representative. Pricing for additional storage, where applicable, is listed under IBM's GSA schedule, or via our public website, or if guaranteed future purchase pricing if included in a transaction document at time of SaaS subscription purchases.

SoftLayer

SoftLayer enables customers to provision additional storage space as needed via the customer portal. Customer has certain disk limitations per server depending on whether they utilize all available drives, but any off-server storage options can be easily provisioned on-demand.

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).

IaaS Response:

IBM Cloud offers a variety of monitoring tools that can be used by authorized personnel to perform essential operational tasks, as needed to ensure continuous and secure operation of your cloud hosted systems. Examples of some of the monitoring tools and services include the following:

- IBM Cloud Monitoring service: To collect, visualize and retain metrics, and define rules and alerts that notify clients of conditions that require attention.
- Grafana as means to use Visualization to monitor your environment.
- New Relic: Software analytics product for application performance monitoring (APM), also it provides data visualization.
- IBM Cloud Event Management service: Used for real-time incident management for your services, applications, and infrastructure.
- IBM Cloud Application Performance Management (APM) solution allows the State to actively monitor and manage your application infrastructure performance in order to quickly respond and ensure optimal experience for your users.
- Email security and monitoring: Cloud-based, hosted security services that can be selected individually or in any combination to help fend off threats that arrive in your organization's email system or enter through the web. The services protect data from email or web-based security threats such as malware, identity theft, and phishing scams by proactively monitoring web traffic.
- DDOS Monitoring / Management:

  IBM Cloud offers DDOS services via the F5 BIG-IP Virtual Edition (VE) available as part of IBM Cloud for VMWare solutions. It provides Distributed Denial of Service (DDoS) mitigation capabilities as part of the Better and Best BIG-IP Licensing options.
- DevOps Monitoring tools, such as Activity Tracker, Availability Monitoring, DevOps Insights, Log Analysis, and Monitoring.
- IBM Geospatial Analytics for IBM Cloud allows monitoring moving devices from a client's application in the IBM Cloud.
- IBM enforces logging and monitoring of actions taken by IBM privileged admins. To the extent that these actions may impact the customers, they are available to you through your service tickets and the device management history viewable through the web portal and API.
- IBM provides audit logs for authentication and portal/API driven actions taken by the State's users.

PaaS Response:

PaaS monitoring tools include Activity Tracker, Alert Notification, Availability Monitoring, Event Management, and Monitoring, which can all be provisioned from the IBM Cloud catalog.

SaaS Response:

IBM SaaS Operations Monitors the applications for all aspects of the Systems Management Processes. This level of monitoring is not provided to our customers as IBM is managing the application based on our internal processes.

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

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

IaaS Response:

IBM Cloud IaaS offers a free IBM Cloud Lite Account that is available at bluemix.net. There are roughly 30 Lite services included in this trial and it is not time-bound.

The Lite Account could be a great platform to implement a Proof of Concept or install some of the State's applications for the purpose of testing the offerings available for you on IBM Cloud, or as needed to enable advanced features in your applications.

IBM offers many free of charge services to enable various categories of cloud skills that you will need to manage and operate your cloud solution.

We can deliver on-site architectural whiteboard sessions, Hackathons, and Design Thinking session led by IBM SMEs. Our on-site developer engagement and enablement services are complemented by a rich IBM Cloud Architecture Center that provides solution templates and cloud reference architectures for jump starting the State's cloud application development.

Some of the example of trainings we can provide to the State include the following:

- Training on specific IBM Cloud IaaS features.
- Training for DBaaS administrators or database PaaS administration.
- Training leading to Certifications for IBM Cloud, for example:
  - IBM Certified Solution Advisor - Cloud Reference Architecture V5.
  - IBM Certified Solution Architect - Cloud Platform.
  - IBM Certified Application Developer - Cloud Platform.
  - IBM Certified Advanced Application Developer - Cloud Platform.

PaaS Response:

A free IBM Cloud Lite Account is available at bluemix.net. There are roughly 30 Lite services included in this trial and it is not time-bound. A list of free training is provided in question 8.17.3.

SaaS Response:

There is no established trial period for most IBM SaaS applications. However, some editions do provide trial, or beta offerings. Proof of concepts are considered on a case by case basis.

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.

IaaS Response:

IBM Cloud provides Lite account (free) that our clients can set up to explore IBM Cloud Offerings. That account does not have any time limits, no credit card is required, and it includes many services that you can evaluate. Any additional services that are not included through IBM Cloud Lite can be activated for a limited time.

IBM Cloud Organization would be happy to work with the State to define a Proof of Concept that would demonstrate how some of your critical business capability can be deployed on the cloud and benefit from cloud offerings.

Example use cases for PoCs could include the following:

- IBM Cloud Lite account (free).
- IBM SkyTap offering.
- Semi-production PoC environment on IBM Cloud for VMWare.
- IBM Apprendra for .NET.

Pending the PoC's scope and specific requirements, we would decide on the best fit for a specific PoC platform, as needed to accomplish the agreed-upon PoC objectives.

PaaS Response:

Testing or PoCs for PaaS can be done through the IBM Cloud Lite account and any additional services that are not included through IBM Cloud Lite can be activated for a limited time.

SaaS Response:

There is no established trial period for most IBM SaaS applications. However, some editions so provide trial or beta offerings. Proof of concepts are considered on a case by case basis.

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

IaaS Response:

IBM will be pleased to arrange training on the use of the IBM Cloud Customer Portal and specific Cloud IaaS features.

IBM will also provide a free-of-charge training to educate the State's developers on how to use IBM Cloud and Watson services to build cloud-native and cognitive applications.

In addition, as indicated in the PaaS Response below: IBM provides a number of online resources that cover abundance of information on all aspects of designing, deploying, managing, and maintaining solutions deployed on IBM Cloud infrastructure.

The IBM Developers Community, which the State can join without limitations, will provide you with the latest tools and tutorials, as needed to address questions you

may have. As the member of that community, you can collaborate with other members on any essential topic to ensure successful operations of your systems.

PaaS Response:

Basic support, including ticketing, is available with all IBM PaaS accounts. Additionally, there are a number of free resources for support and training including:

- IBM Cloud Documentation.
- IBM Cloud on Stack Overflow.
- IBM Cloud on GitHub.
- IBM DeveloperWorks: tutorials, tools, and communities for developers.
- IBM Cloud Tutorials: available through the IBM Cloud console in the Documentation section.
- IBM Open Badges: take IBM learning modules and earn IBM Cloud badges though Acclaim.
- IBM Redbooks for Cloud.

SaaS Response:

Beyond the managed SaaS application, IBM can provide a full range of implementation and consulting services to help our customers make effective use of our SaaS applications. These include:

- Business Analysts to define the future state process and implementation project.
- Project Management for implementation projects.
- Application experts to help configure and implement business processes.
- Training and premium support.

Online demonstrations and tutorials are available for some of offerings where appropriate. Through our DeveloperWorks program we offer on line training videos. Our User Groups are also a key source for educational opportunities.

8.18 (E) INTEGRATION AND CUSTOMIZATION

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

IaaS Response:

IBM Cloud provides many offerings that facilitate integration with other applications and systems, and that enable advanced features, as needed, to conduct business and maintain relationships in the digital era.

Some examples include IBM App Connect, IBM Cloud Integration Service, Box, Searchly, Twilio, Ustream, PubNub, API Connect, and Istio.

IBM Searchly on IBM Cloud is a hosted web search service powered by Elasticsearch. Searchly aims to provide great search experience with advanced

features and APIs of ElasticSearch as well as easy integration (built-in crawler and data importers) and search analytics.

IBM Digital Business Assistant, which is based on IBM Watson Conversation services and on the new Watson Assistant, provides automated connectors to a variety of web sources such MailChimp, SurveyMonkey, Box, Insightly, Google Forms, Gmail, Salesforce.com, SugarCRM, and many other SaaS offerings as well as web sites.

Watson Assistant makes it possible to add a natural language interface to the State's applications to automate interactions with your users. Common applications include virtual agents and chat bots that can integrate and communicate on any channel or device.

The State can train Watson Assistant service through an easy-to-use web application, designed so you can quickly build natural conversation flows between your apps and users, and deploy scalable, cost-effective solutions.

IBM Cloud Information Server provide data integration and governance as a service. It offers the rich features of an on-premises data integration product deployment without the cost and complexity of deploying the infrastructure.

IBM Watson Conversation API or the Voice Agent with Watson provide means to understanding natural language from application users.

The IBM Cloud also provides several IBM Watson Data Kits. For example, Rach kit provide pre-trained data from different industries and domains, offered as APIs for easy integration into your cognitive solution. As a result, the State can deploy a public service application that tracks and informs about specialized enrollment terms of a particular program for example. Or you can deploy an application in support of tourism to suggest points of interest for a particular type of user.

IBM Cloud provides many offerings that allows shortening the delivery of cognitive solutions from months to weeks, thereby lowering the overall solution implementation cost.

Please visit the IBM Cloud Offering Catalog for the listing of the solutions that can facilitate integrations with other applications and that provides easy-to-use software solutions meant to benefit the State's operations.

PaaS Response:

Same as IaaS. The IBM PaaS toolset provides a number of prebuilt connectors to popular cloud and hybrid solutions and also provides the capability for clients to add their own connectors. Additionally, IBM embraces open source technology and includes integrations to many open source tools.

SaaS Response:

IBM is an industry leader in integration and integration tooling based on open standards. Many of our IBM SaaS products are pre-integrated due to complementary functionality. Many third party SaaS applications that you may already have, from both Business Partners and Competitors, are pre-integrated to build on the IBM SaaS Offerings. IBM commonly assists our customers in developing integration services where they do not currently exist.

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

IaaS Response:

While most of IBM Cloud IaaS standard Offerings can be deployed as fast as in minutes on demand, IBM has several organizations that support IBM Cloud operations and can be engaged as part of a separate SOW to address the Purchasing Entities' specific needs for customization and personalization of standard solutions. We have methodology, resources, technology and Managed Services available for you to accomplish the most challenging customization and personalization goals.

For instance, IBM's consultancy known as IBM Cloud Garage, can assist in rapid identification and implementation of specific customization and personalization features; The Garage can design, prove, and build the right innovative, scalable applications on IBM Cloud for the client's target market. The IBM Cloud Garage also helps to build modern hybrid cloud platforms and it enables and trains our customers to adopt quickly customized cloud solutions.

PaaS Response:

Same as IaaS response.

SaaS Response:

Most SaaS applications have abundant personalization features to tailor the user experience and function based on our customer's requirements. This customization is dependent on business functionality of the SaaS application. Many IBM SaaS products, such as Business Process Manager or Cast Iron, are specifically designed to implement custom flows and/or integrations.

8.19 (E) MARKETING PLAN

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

IBM offers assigned face-to-face or telephone/web-based customer service representatives in all 50 states (depending on customer preference and geography). Additionally, many of our IaaS, PaaS and SaaS solutions as well as others from business partners that add value to these IBM solutions can be evaluated and procured directly via our Cloud Marketplace off of IBM's website.

We have marketing teams that focus on the government and education sector that can help NASPO and Participating Entities get this information out to various stakeholders.

We also have other solutions from IBM that also build upon these cloud solutions that are being marketed to these Participating Entities. For example, we have a Smarter Buildings solution that combines IBM software and services to help reduce the energy and

management costs for buildings on government and university campuses that runs on top of our SoftLayer IaaS solution.

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

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

IaaS Response:

IBM is among the leading IT services providers in the world and offers a full range of IT, security, and business consulting services to assist clients with improving efficiency and agility. IBM also offers a full range of professional and managed services for assistance with standing up, configuring, and managing the State's cloud environments. All of these services are available pre- and post-sale, and for on premises and on IBM Cloud. IBM also offers these services for your environments, which may be on other provider's clouds.

IBM provides hundreds of US state, local, and national government clients with the highest quality services across a wide range of capabilities including traditional hosting, single-tenant private clouds, multi-tenant clouds, and a variety of managed services including infrastructure, security, and workload migration. IBM provides these services across Agency, IBM, and even third party data centers. Our cloud capabilities extend beyond physical infrastructure (IaaS) as we also provide Platform (PaaS) and Software (SaaS) offerings.

Some of the key Services we offer to our customers are as follows:

- Application Lifecycle Services.
- Business Resiliency Services.
- Business Strategy and Design Services.
- Cloud Services.
- Design Thinking and Agile Methodologies Workshops.
- Digital Workplace Services.
- Migration Planning and Services.
- Network Services.
- Business Process and Operations.
- Security Services.
- Technology Services.

PaaS Response:

Same as IaaS response.

SaaS Response:

IBM offers both packaged deliverable services and hourly services in order to support our SaaS applications. More complex and transformational projects can also be delivered through our consulting and application delivery services teams.

8.22 (E) SUPPORTING INFRASTRUCTURE

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

IaaS Response:

IBM Cloud IaaS provides all infrastructure components, as needed, to support, operate, and manage our solutions and various cloud deployment models offered as part of our infrastructure.

PaaS Response:

IBM PaaS provides all the infrastructure that is required for running and managing solutions. IBM PaaS also provides devOps tools the Purchasing Entity can use to develop, build, and deploy solutions. There is no additional information to install.

SaaS Response:

Most IBM SaaS applications are delivered via browser or mobile applications technology. They do not require additional infrastructure beyond the user device capable of supporting these browser or mobile interfaces.

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

IaaS Response:

IBM Cloud IaaS platform provides all infrastructure components in support of in scope cloud deployment models. In circumstances where a new customer infrastructure is needed, customers have a choice to procure infrastructure components from the IBM Cloud UI, such as, Bare Metal servers or Virtual Servers, for example. The provisioning of those components will be done in automated manners, and the installation cost will be included in the service charges.

As an example, IBM Cloud for VMware Solutions is provided as an infrastructure solution in the IBM Cloud catalog. The IBM Cloud for VMware Solutions console is the interface where you order and manage your deployments. Each deployment is managed as an instance in the console. To deploy a flexible and customizable VMware virtualized platform that best fits your workload needs, you would order a VMware vCenter Server instance.

When you order a vCenter Server instance, you can also order additional services. Based on your selected configuration for the instance and add-on services, the estimated cost is instantly generated and displayed in IBM Cloud UI.

Once you have completed the details of the order, and submitted it, the deployment of the ordered instance and selected features start automatically. You receive confirmation that the order is being processed and you can check the status of the deployment by viewing the instance details.

Optionally, IBM Cloud offers installation services to assist in more complex or custom solution deployments.

PaaS Response:

Installation is not required.

SaaS Response:

Most IBM SaaS applications are delivered via browser or mobile applications technology. They do not require additional infrastructure beyond the user device capable of supporting these browser or mobile interfaces. It is assumed that the customer is responsible for end user devices and network costs.

Data Security and Privacy Principles for IBM Cloud Services

The technical and organizational measures provided in this Data Security and Privacy attachment (DSP) apply to IBM Cloud Services, including any underlying applications, platforms, and infrastructure components operated and managed by IBM in providing the Cloud Service (components), except where Client is responsible for security and privacy and otherwise specified in a transaction document (TD). Client is responsible for: a) determining whether the Cloud Service is suitable for Client's use and; b) implementing and managing security and privacy measures for elements not provided and managed by IBM within the Cloud Service described in applicable Attachments and TDs (such as systems and applications built or deployed by Client upon an Infrastructure as a Service offering, or Client end-user access control to Software as a Service offerings). The measures implemented and maintained by IBM within each Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2 or both.

1. Data Protection

a. Security and privacy measures for each Cloud Service are designed in accordance with IBM's secure engineering and privacy-by-design practices to protect Content input into a Cloud Service, and to maintain the availability of such Content pursuant to the Agreement, including applicable Attachments and TDs. Client is the sole controller for any personal data included in the Content and appoints IBM as a processor to process such personal data (as those terms are defined in Regulation (EU) 2016/679, General Data Protection Regulation). IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and subprocessors, and only to the extent necessary to deliver the Cloud Service, unless otherwise specified in a TD.

b. IBM will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization.

c. Upon request, IBM will provide evidence of stated compliance and accreditation, such as certificates, attestations, or reports resulting from accredited independent third-party audits, such as ISO 27001, SSAE SOC 2, and other industry standards as specified in a TD. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain the Cloud Service's stated compliance and accreditation.

d. Additional security and privacy information specific to a Cloud Service may be available in the relevant TD or other standard documentation to aide in Client's initial and ongoing assessment of a Cloud Service's suitability for use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. IBM will direct Client to available standard documentation if asked to complete Client-preferred questionnaires or forms and Client agrees such documentation will be utilized in lieu of any such request. IBM may charge an additional fee to complete any Client-preferred questionnaires or forms or to provide consultation to Client for such purposes.

2. Security Policies

a. IBM will maintain and follow IT security policies and practices that are integral to IBM's business and mandatory for all IBM employees. The IBM CIO will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

b. IBM will review its IT security policies at least annually and amend such policies as IBM deems reasonable to maintain protection of Cloud Services and Content processed therein.

c. IBM will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly owned IBM subsidiaries. In accordance with IBM internal process and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by IBM. Each IBM company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. IBM employees will complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security policies, as set out in IBM's Business Conduct Guidelines. Additional policy and process training will be provided to persons granted administrative access to Cloud Service components that is specific to their role within IBM's operation and support of the Cloud Service, and as required to maintain compliance and certifications stated in the relevant TD.

3. Security Incidents

a. IBM will maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notification terms of the Agreement.

b. IBM will investigate unauthorized access and unauthorized use of Content of which IBM becomes aware (security incident), and, within the Cloud Service scope, IBM will define and execute an appropriate response plan. Client may notify IBM of a suspected vulnerability or incident by submitting a technical support request.

c. IBM will notify Client without undue delay upon confirmation of a security incident that is known or reasonably suspected by IBM to affect Client. IBM will provide Client with reasonably requested information about such security incident and the status of any IBM remediation and restoration activities.

4. Physical Security and Entry Control

a. IBM will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into IBM facilities used to host the Cloud Service (data centers). Auxiliary entry points into data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

b. Access to data centers and controlled areas within data centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a data center and controlled areas will be logged, and such logs will be retained for not less than one year. IBM will revoke access to controlled data center areas upon separation of an authorized employee. IBM will follow formal documented separation procedures that include, but are not limited to, prompt removal from access control lists and surrender of physical access badges.

c. Any person duly granted temporary permission to enter a data center facility or a controlled area within a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

d. IBM will take precautions to protect the Cloud Service's physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

5. Access, Intervention, Transfer and Separation Control

a. IBM will maintain documented security architecture of networks managed by IBM in its operation of the Cloud Service. IBM will separately review such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense-in-depth standards prior to implementation. IBM may use wireless networking technology in its maintenance and support of the Cloud Service and associated components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to Cloud Service networks. Cloud Service networks do not use wireless networking technology.

b. IBM will maintain measures for a Cloud Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. IBM will maintain appropriate isolation of its production and non-production environments, and, if Content is transferred to a non-production environment, for example in order to reproduce an error at Client's request, security and privacy protections in the non-production environment will be equivalent to those in production.

c. To the extent described in the relevant TD, IBM will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, and FTPS, for Client's secure transfer of Content to and from the Cloud Service over public networks.

d. IBM will encrypt Content at rest when specified in a TD. If the Cloud Service includes management of cryptographic keys, IBM will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

e. If IBM requires access to Content, it will restrict such access to the minimum level required. Such access, including administrative access to any underlying components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorized IBM personnel following the principles of segregation of duties. IBM will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or the request of authorized IBM personnel, such as the account owner's manager.

f. Consistent with industry standard practices, and to the extent natively supported by each component managed by IBM within the Cloud Service, IBM will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

g. IBM will monitor use of privileged access and maintain security information and event management measures designed to: a) identify unauthorized access and activity; b) facilitate a timely and appropriate response; and c) enable internal and independent third-party audits of compliance with documented IBM policy.

h. Logs in which privileged access and activity are recorded will be retained in compliance with IBM's worldwide records management plan. IBM will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

i. To the extent supported by native device or operating system functionality, IBM will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

6. Service Integrity and Availability Control

a. IBM will: a) perform security and privacy risk assessments of its Cloud Services at least annually; b) perform penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter; c) enlist a qualified independent third-party to perform penetration testing at least annually; d) perform automated management and routine verification of underlying components' compliance with security configuration requirements; and e) remediate identified vulnerabilities or noncompliance with its security

configuration requirements based on associated risk, exploitability, and impact. IBM will take reasonable steps to avoid Cloud Service disruption when performing its tests, assessments, scans, and execution of remediation activities.

b. IBM will maintain policies and procedures designed to manage risks associated with the application of changes to its Cloud Services. Prior to implementation, changes to a Cloud Service, including its systems, networks, and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Cloud Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

c. IBM will maintain an inventory of all information technology assets used in its operation of the Cloud Service. IBM will continuously monitor and manage the health, including capacity, and availability of the Cloud Service and underlying components.

d. Each Cloud Service will be separately assessed for business continuity and disaster recovery requirements pursuant to documented risk management guidelines. Each IBM Cloud Service will have, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for the Cloud Service, if provided, will be established with consideration given to the Cloud Service's architecture and intended use, and will be described in the relevant TD. Physical media intended for off-site storage, if any, such as media containing Cloud Service backup files, will be encrypted prior to transport.

e. IBM will maintain measures designed to assess, test, and apply security advisory patches to the Cloud Service and its associated systems, networks, applications, and underlying components within the Cloud Service scope. Upon determining that a security advisory patch is applicable and appropriate, IBM will implement the patch pursuant to documented severity and risk assessment guidelines. Implementation of security advisory patches will be subject to IBM change management policy.

Data Processing Addendum

This Data Processing Addendum (DPA) and its applicable DPA Exhibits apply to the Processing of Personal Data by IBM on behalf of Client (Client Personal Data) subject to the General Data Protection Regulation 2016/679 (GDPR) or any other data protection laws identified at http://www.ibm.com/dpa/dpl (together 'Data Protection Laws') in order to provide services (Services) pursuant to the Agreement between Client and IBM. DPA Exhibits for each Service will be provided in the applicable Transaction Document (TD). This DPA is incorporated into the Agreement. Capitalized terms used and not defined herein have the meanings given them in the applicable Data Protection Laws. In the event of conflict, the DPA Exhibit prevails over the DPA which prevails over the rest of the Agreement.

1. Processing

1.1 Client is: (a) a Controller of Client Personal Data; or (b) acting as Processor on behalf of other Controllers and has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Client Personal Data by IBM as Client's subprocessor as set out in this DPA. Client appoints IBM as Processor to Process Client Personal Data. If there are other Controllers, Client will identify and inform IBM of any such other Controllers prior to providing their Personal Data, in accordance with the DPA Exhibit.

1.2 A list of categories of Data Subjects, types of Client Personal Data, Special Categories of Personal Data and the processing activities is set out in the applicable DPA Exhibit for a Service. The duration of the Processing corresponds to the duration of the Service, unless otherwise stated in the DPA Exhibit. The purpose and subject matter of the Processing is the provision of the Service as described in the Agreement.

1.3 IBM will Process Client Personal Data according to Client's documented instructions. The scope of Client's instructions for the Processing of Client Personal Data is defined by the Agreement, and, if applicable, Client's and its authorized users' use and configuration of the features of the Service. Client may provide further legally required instructions regarding the Processing of Client Personal Data (Additional Instructions) as described in Section 10.2. If IBM notifies Client that an Additional Instruction is not feasible, the parties shall work together to find an alternative. If IBM notifies the Client that neither the Additional Instruction nor an alternative is feasible, Client may terminate the affected Service, in accordance with any applicable terms of the Agreement. If IBM believes an instruction violates the Data Protection Laws, IBM will immediately inform Client, and may suspend the performance of such instruction until Client has modified or confirmed its lawfulness in documented form.

1.4 Client shall serve as a single point of contact for IBM. As other Controllers may have certain direct rights against IBM, Client undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from the other Controllers. IBM shall be discharged of its obligation to inform or notify another Controller when IBM has provided such information or notice to Client. Similarly, IBM will serve as a single point of contact for Client with respect to its obligations as a Processor under this DPA.

1.5 IBM will comply with all Data Protection Laws in respect of the Services applicable to IBM as Processor. IBM is not responsible for determining the requirements of laws or regulations applicable to Client's business, or that a Service meets the requirements of any such applicable laws or regulations. As between the parties, Client is responsible for the lawfulness of the Processing of the Client Personal Data. Client will not use the Services in a manner that would violate applicable Data Protection Laws.

2. Technical and organizational measures

2.1 Client and IBM agree that IBM will implement and maintain the technical and organizational measures set forth in the applicable DPA Exhibit (TOMs) which ensure a level of security appropriate to the risk for IBM's scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, IBM reserves the right to modify the TOMs provided that the functionality and security of the Services are not degraded.

3. Data Subject Rights and Requests

3.1 IBM will inform Client of requests from Data Subjects exercising their Data Subject rights (e.g., including but not limited to rectification, deletion and blocking of data) addressed directly to IBM regarding Client Personal Data. Client shall be responsible to handle such requests of Data Subjects. IBM will reasonably assist Client in handling such Data Subject requests in accordance with Section 10.2.

3.2 If a Data Subject brings a claim directly against IBM for a violation of their Data Subject rights, Client will reimburse IBM for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that IBM has notified Client about the claim and given Client the opportunity to cooperate with IBM in the defense and settlement of the claim. Subject to the terms of the Agreement, Client may claim from IBM damages resulting from Data Subject claims for a violation of their Data Subject rights caused by IBM's breach of its obligations under this DPA and the respective DPA Exhibit.

4. Third Party Requests and Confidentiality

4.1 IBM will not disclose Client Personal Data to any third party, unless authorized by the Client or required by law. If a government or Supervisory Authority demands access to Client Personal Data, IBM will notify Client prior to disclosure, unless such notification is prohibited by law.

4.2 IBM requires all of its personnel authorized to Process Client Personal Data to commit themselves to confidentiality and not Process such Client Personal Data for any other purposes, except on instructions from Client or unless required by applicable law.

5. Audit

5.1 IBM shall allow for, and contribute to, audits, including inspections, conducted by the Client or another auditor mandated by the Client in accordance with the following procedures:

a. Upon Client's written request, IBM will provide Client or its mandated auditor with the most recent certifications and/or summary audit report(s), which IBM has procured to regularly test, assess and evaluate the effectiveness of the TOMs, to the extent set out in the DPA Exhibit.

b. IBM will reasonably cooperate with Client by providing available additional information concerning the TOMs, to help Client better understand such TOMs.

c. If further information is needed by Client to comply with its own or other Controllers audit obligations or a competent Supervisory Authority's request, Client will inform IBM in writing to enable IBM to provide such information or to grant access to it.

d. To the extent it is not possible to otherwise satisfy an audit right mandated by applicable law or expressly agreed by the Parties, only legally mandated entities (such as a governmental regulatory agency having oversight of Client's operations), the Client or its mandated auditor may conduct an onsite visit of the IBM facilities used to provide the Service, during normal business hours and only in a manner that causes minimal disruption to IBM's business, subject to coordinating the timing of such visit and in accordance with any audit procedures described in the DPA Exhibit in order to reduce any risk to IBM's other customers.

Any other auditor mandated by the Client shall not be a direct competitor of IBM with regard to the Services and shall be bound to an obligation of confidentiality.

5.2 Each party will bear its own costs in respect of paragraphs a. and b. of Section 5.1, otherwise Section 10.2 applies accordingly.

6. Return or Deletion of Client Personal Data

6.1 Upon termination or expiration of the Agreement IBM will either delete or return Client Personal Data in its possession as set out in the respective DPA Exhibit, unless otherwise required by applicable law.

7. Subprocessors

7.1 Client authorizes the engagement of other Processors to Process Client Personal Data (Subprocessors). A list of the current Subprocessors is set out in the respective DPA Exhibit. IBM will notify Client in advance of any addition or replacement of the Subprocessors as set out in the respective DPA Exhibit. Within 30 days after IBM's notification of the intended change, Client can object to the addition of a Subprocessor on the basis that such addition would cause Client to violate applicable legal requirements. Client's objection shall be in writing and include Client's specific reasons for its objection and options to mitigate, if any. If Client does not object within such period, the respective Subprocessor may be commissioned to Process Client Personal Data. IBM shall impose substantially similar but no less protective data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor initiating any Processing of Client Personal Data.

7.2 If Client legitimately objects to the addition of a Subprocessor and IBM cannot reasonably accommodate Client's objection, IBM will notify Client. Client may terminate the affected Services as set out in the

Agreement, otherwise the parties shall cooperate to find a feasible solution in accordance with the dispute resolution process.

8. Transborder Data Processing

8.1 In the case of a transfer of Client Personal Data to a country not providing an adequate level of protection pursuant to the Data Protection Laws (Non-Adequate Country), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws as set out in the following Sections. If Client believes the measures set out below are not sufficient to satisfy the legal requirements, Client shall notify IBM and the parties shall work together to find an alternative.

8.2 By entering into the Agreement, Client is entering into EU Standard Contractual Clauses as set out in the applicable DPA Exhibit (EU SCC) with (i) each Subprocessor listed in the respective DPA Exhibit that is an IBM affiliate located in a Non-Adequate Country (IBM Data Importers) and (ii) IBM, if located in a Non-Adequate Country, as follows:

a. if Client is a Controller of all or part of the Client Personal Data, Client is entering into the EU SCC in respect to such Client Personal Data; and

b. if Client is acting as Processor on behalf of other Controllers of all or part of the Client Personal Data, then Client is entering into the EU SCC:

(i) as back-to-back EU SCC in accordance with Clause 11 of the EU Standard Contractual Clauses (Back-to-Back SCC), provided that Client has entered into separate EU Standard Contractual Clauses with the Controllers; or

(ii) on behalf of the other Controller(s).

Client agrees in advance that any new IBM Data Importer engaged by IBM in accordance with Section 7 shall become an additional data importer under the EU SCC and/or Back-to-Back SCC.

8.3 If a Subprocessor located in a Non-Adequate Country is not an IBM Data Importer (Third Party Data Importer) and EU SCC are entered into in accordance with Section 8.2, then, IBM or an IBM Data Importer shall enter into Back-to-Back SCC with such a Third Party Data Importer. Otherwise, Client on its own behalf and/or, if required, on behalf of other Controllers shall enter into separate EU Standard Contractual Clauses or Back-to-Back SCC as provided by IBM.

8.4 If Client is unable to agree to the EU SCC or Back-to-Back SCC on behalf of another Controller, as set out in section 8.2 and 8.3, Client will procure the agreement of such other Controller to enter into those agreements directly. Additionally, Client agrees and, if applicable, procures the agreement of other Controllers that the EU SCC or the Back-to-Back SCC, including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability. In case of conflict, the EU SCC and Back-to-Back SCC shall prevail.

9. Personal Data Breach

9.1 IBM will notify Client without undue delay after becoming aware of a Personal Data Breach with respect to the Services. IBM will promptly investigate the Personal Data Breach if it occurred on IBM infrastructure or in another area IBM is responsible for and will assist Client as set out in Section 10.

10. Assistance

10.1 IBM will assist Client by technical and organizational measures for the fulfillment of Client's obligation to comply with the rights of Data Subjects and in ensuring compliance with Clients obligations relating to the security of Processing, the notification and communication of a Personal Data Breach and the Data Protection Impact Assessment, including prior consultation with the responsible Supervisory Authority, if required, taking into account the nature of the processing and the information available to IBM.

10.2 Client will make a written request for any assistance referred to in this DPA. IBM may charge Client no more than a reasonable charge to perform such assistance or an Additional Instruction, such charges to be set forth in a quote and agreed in writing by the parties, or as set forth in an applicable change control provision of the Agreement. If Client does not agree to the quote, the parties agree to reasonably cooperate to find a feasible solution in accordance with the dispute resolution process.

Business Associate Addendum

This Business Associate Addendum ("Addendum") supplements and is made a part of the base agreement, and applicable transaction document(s), between Client and International Business Machines Corporation (IBM) for the services that will be processing protected health information of individuals governed by U.S. laws and regulations (collectively, the "Agreement"). IBM and Client may be referred to individually as a "Party" or collectively as the "Parties." Once accepted electronically, any reproduction made by reliable means (for example, electronic image, photocopy or facsimile) is considered an original.

RECITALS

Client is a "covered entity", as such term is defined by HIPAA (defined below).

Client and IBM are Parties to the Agreement pursuant to which IBM provides certain services to Client. In connection with those services, the Parties anticipate that it may be necessary for IBM to create, receive, maintain, transmit, use, or disclose certain Protected Health Information from, or on behalf of, Client ("Client PHI") that is subject to protection under the privacy, security and breach notification requirements of the Health Insurance Portability and Accountability Act of 1996, as amended, including by the Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act of 2009 ("HITECH Act"), certain regulations promulgated under HIPAA by the United States Department of Health and Human Services at 45 C.F.R. Parts 160 and 164 and certain regulations promulgated pursuant to the HITECH Act (collectively, "HIPAA").

The purpose of this Addendum is to help facilitate the Parties' compliance with the requirements of HIPAA, as applicable when IBM is acting as a business associate of Client.

Client acknowledges that IBM may act in a capacity other than as a business associate and that this Addendum only applies to the extent that IBM is acting as a business associate for Client. Hereinafter, however, IBM will be referred to as "Business Associate."

NOW, THEREFORE, in consideration of the mutual promises and other consideration contained in this Addendum, the delivery and sufficiency of which is hereby acknowledged, the Parties agree as follows:

AGREEMENT

1. Definitions. Unless otherwise provided in this Addendum, capitalized terms have the same meaning as set forth in HIPAA. "Applicable Law" means, in respect of any person, all provisions of constitutions, statutes, rules, regulations, and orders of governmental bodies or regulatory agencies applicable to such person, including, without limitation, HIPAA and state privacy laws and security breach notification laws, and all orders and decrees of all courts and arbitrators in proceedings or actions to which the person in question is a party or by which it or its properties are bound.

2. Applicability. This Addendum shall be applicable solely to Protected Health Information that is Client PHI. Client will not provide Business Associate with access to, or direct Business Associate to create, receive, maintain, transmit, use, or disclose, Client PHI unless a description of the Client PHI, its location and any requirements related to such Client PHI are mutually agreed upon in the applicable transaction document.

3. Minimum Necessary Disclosures. In accordance with HIPAA, Client shall limit its uses, disclosures and requests of Client PHI to Business Associate to the minimum necessary to accomplish the services Business Associate is performing for Client. Business Associate shall further limit its use, disclosures and requests of Client PHI to the minimum necessary Client PHI to perform or have performed the services Business Associate is performing for Client. In each case, Client shall exercise reasonable discretion to determine what constitutes minimum necessary Client PHI.

4. Scope of Use of Client PHI. Business Associate shall not create, receive, maintain, transmit, use, or disclose Client PHI for any purpose other than as permitted or required by this Addendum or as Required By Law; provided that to the extent Business Associate is to carry out Client's obligations under the Privacy Rule as agreed by the Parties in writing, Business Associate will comply with the requirements of the Privacy Rule that apply to Client in the performance of those obligations.

5. Permitted Uses and Disclosures. Unless otherwise limited in this Addendum, in addition to any other uses and/or disclosures permitted or required by this Addendum, Business Associate may:

5.1 create, receive, maintain, transmit, use, and disclose Client PHI as necessary to provide the services and perform its obligations under the Agreement; and

5.2 create, receive, maintain, transmit, use, and disclose Client PHI for the proper management and administration of Business Associate, or to carry out the legal responsibilities of Business Associate, provided that, with respect to disclosures: (i) the disclosures are Required by Law; or (ii) any third party to which Business Associate discloses Client PHI provides written reasonable assurances in advance that: (a) the information will be held confidentially and used or further disclosed only for the purpose for which it was disclosed to the third party; and (b) the third party promptly will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the Client PHI has been compromised.

6. **Safeguards for the Protection of Client PHI.** Business Associate shall (i) use safeguards that are designed to appropriately prevent the use or disclosure (other than as provided for by this Addendum) of Client PHI and (ii) implement administrative, physical and technical safeguards that are designed to reasonably and appropriately protect the confidentiality,

integrity and availability of Electronic Client PHI. If Business Associate agrees at the request of Client to provide customized safeguards, such safeguards shall be documented in applicable statements of work or in comparable contract documents describing the services to be performed. In all cases, Business Associate shall comply with the Security Rule requirements for business associates in 45 C.F.R. Parts 160 and 164 (Subparts A & C).

7. **Reporting of Unauthorized Uses or Disclosures.** In compliance with HIPAA Business Associate shall report to Client:

7.1 any use or disclosure of Client PHI of which Business Associate becomes aware that is not provided for or permitted in this Addendum;

7.2 any Security Incident of which Business Associate becomes aware; provided, however, that the Parties acknowledge and agree that that no additional notice is required by Business Associate to Client for the ongoing existence and occurrence of Unsuccessful Security Incidents. "Unsuccessful Security Incidents" means, without limitation, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use, disclosure, modification or destruction of Client PHI or intentional interference with system operations in an information system that contains Client PHI; and

7.3 any Breach of Unsecured Client PHI of which Business Associate becomes aware, without unreasonable delay and in no case later than 30 days following the discovery by Business Associate of such Breach. Business Associate shall provide Client with written notification of Breach in accordance with 45 C.F.R. § 164.410.

8. **Use of Subcontractors**. Business Associate shall cause each Subcontractor of Business Associate (including, without limitation, a Subcontractor that is an agent under Applicable Law) that creates, receives, maintains, transmits, uses, or discloses Client PHI on behalf of Client to sign a written agreement with Business Associate satisfying the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) and containing at least as restrictive provisions and conditions related to the protection of Client PHI as those that apply to Business Associate under this Addendum.

9. **Authorized Access to and Amendment of Client PHI.** Only to the extent that Business Associate maintains Client PHI in Designated Record Sets, Business Associate shall: (i) within 30 business days of a written request by Client for access to Client PHI about an Individual contained in any Designated Record Set of Client maintained by Business Associate, make available to Client in accordance with 45 C.F.R. § 164.524, all such Client PHI held by Business Associate, including electronic access to Client PHI maintained by Business Associate in electronic form; and (ii) within 30 business days of a written request by Client to amend Client PHI, incorporate any amendments Client makes to Client PHI in accordance with 45 C.F.R. § 164.526. In the event that Business Associate receives a request for access to Client PHI directly from an Individual, Business Associate shall direct the Individual to contact Client directly.

10. **Accounting of Disclosures of Client PHI**. Business Associate shall keep records of disclosures of Client PHI made by Business Associate (the "Disclosure Accounting") during the term of this Addendum in accordance with 45 C.F.R. § 164.528. Business Associate shall provide the Disclosure Accounting to Client within 45 days of receiving a written request therefor from Client. Business Associate shall comply with, and assist Client in compliance with, additional requirements of 42 U.S.C. § 13405(c), if and when applicable. In the event that Business Associate receives a request for a Disclosure Accounting of Client PHI directly from an Individual, Business Associate shall direct the Individual to contact Client directly.

11. **Health and Human Services.** Business Associate shall make its internal practices, books and records related to the use and disclosure of Client PHI under the Agreement and this Addendum available to Secretary of the Department of Health and Human Services for the purpose of determining Client's compliance with 45 C.F.R. § 164.500 et seq.

12. **Client Responsibilities.** Client warrants that it has obtained and will obtain any consents, Authorizations, and/or other legal permissions required under HIPAA and other Applicable Law for the disclosure of Client PHI to Business Associate. Client shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of Client PHI under this Addendum. Client shall not agree to any restriction on the creation, receipt, maintenance, transmission, use, or disclosure of PHI under 45 C.F.R. § 164.522 that restricts Business Associate's creation, receipt, maintenance, transmission, use, or disclosure of Client PHI under this Agreement unless such restriction is Required By Law or Business Associate grants its written consent to such restriction, which consent shall not be unreasonably withheld.

13. **Future Protections of Client PHI.** Upon the expiration or earlier termination of this Addendum for any reason, if feasible, Business Associate shall return to Client, or, at Client's direction, destroy, all Client PHI in any form. If Business Associate determines that such return or destruction is not feasible, Business Associate shall extend the protections of this Addendum to the Client PHI and shall limit further creation, receipt, maintenance, transmission, use, or disclosure to those purposes that make the return or destruction of the Client PHI infeasible.

14. **Termination.** Either Party (the "Non-Breaching Party") may terminate this Addendum upon 30 days' prior written notice to the other party (the "Breaching Party") in the event that the Breaching Party materially breaches this Addendum and such breach is not cured to the reasonable satisfaction of the Non-Breaching Party within such 30-day period. In the event of termination of this Addendum, either Party may terminate those portions of the Agreement, and only those portions of the Agreement, that require Business Associate to create, receive, maintain, transmit, use, or disclose Client PHI, in accordance with and subject to any rights to cure and payment obligations specified in the Agreement.

15. **Effect on Agreement.** This Addendum is not intended to, nor shall it be construed to, reduce or diminish any of Business Associate's or Client's obligations under the Agreement. Accordingly, except as set forth in section entitled "Termination" or to

the extent expressly inconsistent with this Addendum, all other terms of the Agreement shall remain in full force and effect and shall not be modified, diminished, or reduced hereby. In the event of a conflict between this Addendum and the agreement, including applicable transaction documents, with respect to the privacy and security of Client PHI or compliance with HIPAA, the terms more protective of Client PHI shall control. In all other cases, the terms of the Agreement shall control.

16. **No Intended Third Party Beneficiaries.** There are no intended third party beneficiaries under this Addendum.

17. **Independent Contractor Status.** The Parties acknowledge and agree that Business Associate is at all times acting as an independent contractor of Client and not as an agent or employee of Client under this Addendum.

18. **Assignment.** Neither Party may assign this Addendum, in whole or in part, without the prior written consent of the other. Any attempt to do so is void. Neither Party will unreasonably withhold such consent. The assignment of this Addendum, in whole or in part, to any majority-owned subsidiary in the United States or to a successor organization by merger or acquisition does not require the consent of the other. It is not considered an assignment for Business Associate to divest a portion of its business in a manner that similarly affects all of its Clients.

19. **Future Amendments.** Any future amendments to HIPAA affecting the required provisions of business associate agreements are hereby incorporated by reference into this Addendum as if set forth in this Addendum in their entirety, effective on the later of the effective date of this Addendum or such subsequent date as may be specified by HIPAA. No other amendment to this Addendum shall be valid unless agreed to in writing by both Parties.

Cloud Services Agreement

This Cloud Services Agreement (CSA) and applicable Attachments and Transaction Documents (TDs) are the complete agreement regarding transactions under this CSA (together, the "Agreement") under which Client may order Cloud Services. TDs detail the specifics of transactions, such as charges and a description of and information about the Cloud Service. Examples of TDs include statements of work, service descriptions, ordering documents and invoices. Attachments provide supplemental terms that apply to certain types of Cloud Services, such as a trial or beta services. Any conflicting terms in an Attachment or TD that override other parts of this CSA will be identified in the TD or Attachment accepted by the Client and only apply to the specific transaction.

1. Cloud Services

a. A Cloud Service is an IBM offering provided by IBM and made available via a network. Each Cloud Service is described in a TD. Cloud Services are designed to be available 24/7, subject to maintenance. Client will be notified of scheduled maintenance. Technical support and service level commitments, if applicable, are specified in an Attachment or TD.

b. IBM may offer Non-IBM services, or an IBM Cloud Service may enable access to Non-IBM services, that may require acceptance of third party terms identified in the TD. Linking to or use of Non-IBM services constitutes Client's agreement with such terms. IBM is not a party to such third party agreements and is not responsible for such Non-IBM services.

c. Client accepts an Attachment or TD by ordering, enrolling, using, or making a payment for the Cloud Service. When IBM accepts Client's order, IBM provides Client the authorizations specified in the TD.

d. IBM will provide the facilities, personnel, equipment, software, and other resources necessary to provide the Cloud Services and generally available user guides and documentation to support Client's use of the Cloud Services. A Cloud Service may require the use of enabling software that Client downloads to Client systems to facilitate use of the Cloud Service. Client may use enabling software only in connection with use of the Cloud Service and according to any licensing terms if specified in a TD. Enabling software is provided as-is, without warranties of any kind.

e. Client will provide hardware, software and connectivity to access and use the Cloud Service, including any required Client-specific URL addresses and associated certificates.

f. Client may access a Cloud Service only to the extent of authorizations acquired by Client. Client is responsible for use of Cloud Services by any user who accesses the Cloud Service with Client's account credentials. A Cloud Service may not be used in any jurisdiction for unlawful, obscene, offensive or fraudulent Content or activity, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive, or deceptive messages, viruses or harmful code, or violating third party rights. In addition, Client may not use Cloud Services if failure of the Cloud Service could lead to death, bodily injury, or property or environmental damage. Client may not: i) reverse engineer any portion of a Cloud Service; ii) assign or resell direct access to a Cloud Service to a third party outside Client's Enterprise; or iii) combine Cloud Services with Client's value add to create a commercially available Client branded solution that Client markets to its end user customers unless otherwise agreed.

g. A Cloud Service or feature of a Cloud Service is considered "Preview" when IBM makes such services or features available at no charge, with limited or pre-release functionality, or for a limited time to try available functionality (such as beta, trial, no-charge, or preview designated Cloud Services). Preview services are excluded from available service level agreements. A Preview service may not be covered by support and IBM may change or discontinue a Preview service at any time and without notice. IBM is not obligated to release a Preview service or make an equivalent service generally available.

2. Content and Data Protection

a. Content consists of all data, software, and information that Client or its authorized users provides, authorizes access to, or inputs to the Cloud Service. Use of the Cloud Service will not affect Client's ownership or license rights in such Content. IBM, its affiliates, and contractors of either, may access and use the Content solely for the purpose of providing and managing the Cloud Service. IBM will treat all Content as confidential by not disclosing Content except to IBM employees and contractors and only to the extent necessary to deliver the Cloud Service.

b. Client is responsible for obtaining all necessary rights and permissions to enable, and grants such rights and permissions to, IBM, its affiliates, and contractors of either, to use, provide, store and otherwise process Content in the Cloud Service. This includes Client making necessary disclosures and obtaining consent, if required, before providing individuals' information, including personal or other regulated data in such Content. If any Content could be subject to governmental regulation or may require security measures beyond those specified by IBM for a Cloud Service, Client will not input, provide, or allow such Content unless specifically permitted in the terms of the relevant TD or unless IBM has otherwise first agreed in writing to implement additional security and other measures.

c. IBM's Data Security and Privacy Principles for IBM Cloud Services (DSP), at http://www.ibm.com/cloud/data-security, apply for generally available Cloud Service offerings. Specific security features and functions of a Cloud Service may be provided in an Attachment and TDs. Client is responsible to assess the suitability of each Cloud Service for Client's intended use and Content and to take necessary actions to order, enable, or use available data protection features appropriate for the Content being used with a Cloud Service. By using the Cloud Service, Client accepts responsibility for use of the Cloud Services, and acknowledges that it meets Client's requirements and processing instructions to enable compliance with applicable laws.

d. IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and applicable DPA Exhibit(s) apply to personal data contained in Content, if and to the extent: i) the European General Data Protection Regulation (EU/2016/679); or ii) other data protection laws identified at www.ibm.com/dpa/dpl apply.

e. IBM will return or remove Content from IBM computing resources upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request. IBM may charge for certain activities performed at Client's request (such as delivering Content in a specific format). IBM does not archive Content, however some Content may remain in Cloud Service backup files until expiration of such files as governed by IBM's backup retention practices.

f. Upon request by either party, IBM, Client or affiliates of either, will enter into additional agreements as required by law in the prescribed form for the protection of regulated personal data included in Content. The parties agree (and will ensure that their respective affiliates agree) that such additional agreements will be subject to the terms of the Agreement.

3. Changes

a. Client acknowledges that IBM may modify: i) a Cloud Service; and ii) the DSP, from time to time at IBM's sole discretion and such modifications will replace prior versions as of the effective date. Updates to a TD (such as a service description or statement of work) will take effect upon a new order or for TDs previously agreed by the Client will take effect upon the change effective date for ongoing services, or upon the renewal date for Cloud Services that automatically renew. The intent of any modification will be to: i) improve or clarify existing commitments; ii) maintain alignment to current adopted standards and applicable laws; or iii) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of a Cloud Service.

b. IBM may withdraw a Cloud Service on 12 months' notice and IBM will continue to provide the Cloud Service for the remainder of Client's unexpired term or work with Client to migrate to another IBM offering. Access to Non-IBM services may be withdrawn at any time.

c. Since this CSA may apply to many future orders, IBM may modify this CSA by providing Client at least three months' written notice. Changes are not retroactive; they apply, as of the effective date, only to new orders, ongoing Cloud Services that do not expire, and renewals. For transactions with a defined renewable contract period stated in a TD, Client may request that IBM defer the change effective date until the end of the current contract period. Client accepts changes by placing new orders or continuing use after the change effective date or allowing transactions to renew after receipt of the change notice. Except as provided above, all changes to the Agreement must be in writing accepted by both parties.

4. Warranties

a. IBM warrants that it provides Cloud Services using commercially reasonable care and skill. The warranty for a Cloud Service ends when the Cloud Service ends.

b. IBM does not warrant uninterrupted or error-free operation of a Cloud Service or that IBM will correct all defects or prevent third party disruptions or unauthorized third party access. These warranties are the exclusive warranties from IBM and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose. IBM warranties will not apply if there has been misuse, modification, damage not caused by IBM, or failure to comply with instructions provided by IBM. Preview services and Non-IBM services are made available under the Agreement as-is, without warranties of any kind. Third parties may provide their own warranties to Client.

5. Charges, Taxes, and Payment

a. Client agrees to pay all applicable charges specified for a Cloud Service and charges for use in excess of authorizations. Charges are exclusive of any customs or other duty, tax, and similar levies imposed by any authority resulting from Client's acquisitions under the Agreement and will be invoiced in addition to such charges. Amounts are due upon receipt of the invoice and payable within 30 days of the invoice date to an account specified by IBM and late payment fees may apply. Prepaid Services must be used within the applicable period. IBM does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid. If IBM has not otherwise committed to pricing during the term of a Cloud Service, then IBM may change charges on thirty days' notice.

b. Client agrees to: i) pay withholding tax directly to the appropriate government entity where required by law; ii) furnish a tax certificate evidencing such payment to IBM; iii) pay IBM only the net proceeds after tax; and iv) fully cooperate with IBM in seeking a waiver or reduction of such taxes and promptly complete and file all relevant documents. Where taxes are based upon the location(s) receiving the benefit of the Cloud Service, Client has an ongoing obligation to notify IBM of such location(s) if different than Client's business address listed in the applicable Attachment or TD.

c. Based on selected billing frequency, IBM will invoice Client the charges due at the beginning of the billing frequency term, except for overage and usage type of charges which will be invoiced in arrears. One time charges will be billed upon acceptance of an order.

6. Liability and Indemnity

a. IBM's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the service that is the subject of the claim, regardless of the basis of the claim. IBM will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings. These limitations apply collectively to IBM, its affiliates, contractors, and suppliers.

b. The following amounts are not subject to the above cap: i) third party payments referred to in the paragraph below; and ii) damages that cannot be limited under applicable law.

c. If a third party asserts a claim against Client that a Cloud Service acquired under the Agreement infringes a patent or copyright, IBM will defend Client against that claim and pay amounts finally awarded by a court against Client or included in a settlement approved by IBM, provided that Client promptly: i) notifies IBM in writing of the claim; ii) supplies information requested by IBM; and iii) allows IBM to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts.

d. IBM has no responsibility for claims based on Non-IBM products and services, items not provided by IBM, or any violation of law or third party rights caused by Client's Content, materials, designs, or specifications.

7. Term and Termination

a. The term of a Cloud Service begins on the date IBM notifies Client that Client can access the Cloud Service. IBM will specify whether the Cloud Service renews automatically, proceeds on a continuous use basis, or terminates at the end of the term. For automatic renewal, unless Client provides written notice to IBM or the IBM Business Partner involved in the Cloud Service not to renew at least 30 days prior to the term expiration date, the Cloud Service will automatically renew for the specified term. For continuous use, the Cloud Service will continue to be available on a month to month basis until Client provides 30 days written notice to IBM or the IBM Business Partner involved in the Cloud Service of termination. The Cloud Service will remain available to the end of the calendar month after such 30 day period.

b. IBM may suspend or limit, to the extent necessary, Client's use of a Cloud Service if IBM determines there is a material breach of Client's obligations, a security breach, violation of law, or breach of the terms set forth in section 1(f). If the cause of the suspension can reasonably be remedied, IBM will provide notice of the actions Client must take to reinstate the Cloud Service. If Client fails to take such actions within a reasonable time, IBM may terminate the Cloud Service. Failure to pay is a material breach.

c. Either party may terminate this CSA: i) without cause on at least one month's notice to the other after expiration or termination of its obligations under the Agreement; or ii) immediately for cause if the other is in material breach of the Agreement, provided the one who is not complying is given notice and reasonable time to comply. Any terms that by their nature extend beyond the Agreement termination remain in effect until fulfilled, and apply to successors and assignees. Termination of this CSA does not terminate TDs, and provisions of this CSA as they relate to such TDs remain in effect until fulfilled or otherwise terminated in accordance with their terms.

d. Client may terminate a Cloud Service on one month's notice: i) at the written recommendation of a government or regulatory agency following a change in either applicable law or the Cloud Services; ii) if IBM's modification to the computing environment used to provide the Cloud Service causes Client to be noncompliant with applicable laws; or iii) if IBM notifies Client of a modification that has a material adverse effect on Client's use of the Cloud Service, provided that IBM will have 90 days to work with Client to minimize such effect. In the event of such termination, IBM shall refund a portion of any prepaid amounts for the applicable Cloud Service for the period after the date of termination. If the Agreement is terminated for any other reason, Client shall pay to IBM, on the date of termination, the total amounts due per the Agreement. Upon termination, IBM may assist Client in transitioning Client's Content to an alternative technology for an additional charge and under separately agreed terms.

8. Governing Laws and Geographic Scope

a. Each party is responsible for complying with: i) laws and regulations applicable to its business and Content; and ii) import, export and economic sanction laws and regulations, including defense trade control regime of any jurisdiction, including the International Traffic in Arms Regulations and those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users.

b. Both parties agree to the application of the laws of the State of New York, United States, without regard to conflict of law principles. The rights and obligations of each party are valid only in the country of Client's business address. If Client or any user exports or imports Content or use of any portion of the Cloud Service outside the country of Client's business address, IBM will not serve as the exporter or importer, except as required by data protection laws. If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect. Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under the Agreement.

9. General

a. IBM is an independent contractor, not Client's agent, joint venturer, partner, or fiduciary, and does not undertake to perform any of Client's regulatory obligations or assume any responsibility for Client's business or operations. IBM is an information technology provider only. Any directions, suggested usage, or guidance provided by IBM or a Cloud Service does not constitute medical, clinical, legal, accounting, or other licensed professional advice. Client and its authorized users are responsible for the use of the Cloud Service within any professional practice and should obtain their own expert advice. Client is responsible for its use of IBM and Non-IBM products and services. Each party is responsible for determining the assignment of its and its affiliates personnel, and their respective contractors, and for their direction, control, and compensation.

b. IBM maintains a robust set of business conduct and related guidelines covering conflicts of interest, market abuse, anti-bribery and corruption, and fraud. IBM and its personnel comply with such policies and require contractors to have similar policies.

c. IBM, its affiliates, and contractors of either, may, wherever they do business, store and otherwise process business contact information (BCI) of Client, its personnel and authorized users, for example, name, business telephone, address, email, and user ID for business dealings with them. Where notice to or consent by the individuals is required for such processing, Client will notify and obtain such consent. The IBM Privacy Statement at https://www.ibm.com/privacy/ provides additional details with respect to BCI and Account Data described below.

d. Account Data is information, other than Content and BCI, that Client provides to IBM to enable Client's use of a Cloud Service or that IBM collects using tracking technologies, such as cookies and web beacons, regarding Clients use of a Cloud Service. IBM, its affiliates, and contractors of either, may use Account Data for example to enable product features, administer use, personalize experience, and otherwise support or improve use of the Cloud Service.

e. IBM Business Partners who use or make available IBM Cloud Services are independent from IBM and unilaterally determine their prices and terms. IBM is not responsible for their actions, omissions, statements, or offerings.

f. Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other. Assignment of IBM rights to receive payments or assignment by IBM in conjunction with the sale of the portion of IBM's business that includes a service is not restricted.

g. This CSA applies to IBM and Client and their respective Enterprise companies who acquire Cloud Services under this CSA. The parties shall coordinate the activities of their own Enterprise companies under the Agreement. Enterprise companies include: i) companies within the same country that Client or IBM control (by owning greater than 50% of the voting shares); and ii) any other entity that controls, is controlled by or is under common control with Client or IBM and has signed a participation agreement.

h. All notices under the Agreement must be in writing and sent to the business address specified for the Agreement, unless a party designates in writing a different address. The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing. Any reproduction of the Agreement made by reliable means is considered an original. The Agreement supersedes any course of dealing, discussions or representations between the parties.

i. No right or cause of action for any third party is created by the Agreement or any transaction under it. Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose. Neither party is responsible for failure to fulfill its non-monetary obligations due to causes beyond its control. Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations. Where approval,

acceptance, consent, access, cooperation or similar action by either party is required, such action will not be unreasonably delayed or withheld.

j. IBM may use personnel and resources in locations worldwide, including contractors to support the delivery of the Cloud Services. IBM may transfer Content, including personal data, across country borders. A list of countries where Content may be processed for a Cloud Service is described in the TD. IBM is responsible for the obligations under the Agreement even if IBM uses a contractor and will have appropriate agreements in place to enable IBM to meet its obligations for a Cloud Service.

k. IBM may offer additional customization, configuration or other services to support Cloud Services, as detailed in a TD.

Agreed to:	Agreed to:
Client Company Name:	IBM Company:
By _____	By _____
Authorized Signature	Authorized Signature
Title:	Title:
Name (type or print):	Name (type or print):
Date:	Date:
Client number:	Agreement number:
Enterprise number:	
Client address:	IBM address: