

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) Amazon

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR INFRASTRUCTURE AS A SERVICE (IaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). STATE AGENCIES MUST FIRST:

- A. CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;
- B. CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;
- C. **MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION**^[A1].

1. DEFINITIONS:

- a. "Authorized Persons" means the Service Provider's employees, Contractors, subcontractors or other agents who need to access the State's Data to enable the Service Provider to perform the services required.
- b. "Data Breach" means the unauthorized access that results in the use, disclosure, destruction, modification, loss or theft of the State's unencrypted Personal Data or Non-Public Data.
- c. "Individually Identifiable Health Information" means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- d. "Infrastructure-as-a-Service" (IaaS) means the capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).
- e. "Non-Public Data" means data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, regulation or policy from access by the general public as public information.
- f. "Personal Data" means data that includes information relating to a person that identifies the person by name and has any of 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.
- g. "Protected Health Information" (PHI) means Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.
- h. "State Data" means all data created or in any way originating with the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, the Service Provider's hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Service Provider.
- i. "State Identified Contact" means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.
- j. "Security Incident" means the **potentially unauthorized access to Personal Data or Non-Public Data the Service Provider believes could reasonably result in** ^[A2] the use, disclosure or theft of the State's unencrypted Personal Data or Non-Public Data within the possession or control of the Service Provider. A Security Incident may or may not turn into a Data Breach.

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) Amazon

- k. "Service Level Agreement" (SLA) means a written agreement between both the State and the Service Provider that is subject to the terms and conditions in this document that unless otherwise agreed to [A3] includes (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) security responsibilities and notice requirements, how disputes are discovered and addressed, and (6) any remedies for performance failures.
- l. "Service Provider" means the Contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Contract.
- m. "Statement of Work" (SOW) means a written statement in a solicitation document or Contract that describes the State's service needs and expectations.

2. DATA OWNERSHIP:

The State will own all right, title and interest in State Data that is related to the services provided by this Contract. The Service Provider shall not access State user accounts or State 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 Contract, (4) at the State's written request or (5) as required by law.

3. DATA PROTECTION:

Protection of personal privacy and data shall be an integral part of the business activities of the Service Provider. Requirements and responsibilities for security of State Data shall be set forth in the SOW and/or SLA to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, tThe Service Provider shall safeguard the confidentiality, integrity and availability of State information within its control and comply with the following conditions: [A4]

- a. In addition to the Compliance with Statutes and Regulations provisions set forth in the General Provisions – Information Technology
 - i. The California Information Practices Act [A5] (Civil Code Sections 1798 et seq).
 - ii. NIST Special Publication 800-53 Revision 4 or its successor.
 - iii. Privacy provisions of the Federal Privacy Act of 1974.
- b. All State Data obtained by the Service Provider within its control in the performance of this Contract shall become and remain the property of the State [A6].
- c. Unless otherwise stipulated in the SOW and/or SLA, Personal Data and Non-Public Data shall be encrypted at rest, in use, and in transit with controlled access. The SOW and/or SLA [A7] will specify which party is responsible for encryption and access control of the State Data for the service model under Contract. If the SOW and/or SLA and the Contract are silent, then the State is responsible for encryption and access control.
- d. Unless otherwise stipulated in the SOW and/or SLA, it is the State's responsibility to identify data it deems as Non-Public Data to the Service Provider. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.
- e. Unless otherwise stipulated in the SOW and/or SLA, [A8]aAt no time shall any data or processes — which either belong to or are intended for the use of State or its officers, agents or employees — be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State.

4. DATA LOCATION:

The Service Provider shall provide its services to the State and its end users solely from data centers in the continental United States. Storage of State Data at rest shall be located solely in data centers [A9] in the continental United States. The Service Provider shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Service Provider shall permit its personnel and contractors to access State Data remotely only as required to provide technical support, or as necessary for the delivery of the services to the State and/or

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) Amazon

maintenance of the services. The Service Provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this Contract.

5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

Unless otherwise stipulated [A10] in the SOW and/or SLA, tThe Service Provider shall inform the State of any Security Incident or Data Breach related to State Data within the possession or control of the Service Provider and related to the service provided under this Contract.

- a. Security Incident Reporting Requirements: Unless otherwise stipulated in the SOW and/or SLA, the Service Provider shall immediately report a Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA. [A11]
- b. Breach Reporting Requirements: Unless otherwise stipulated in the SOW and/or SLA, if the Service Provider has actual knowledge of a confirmed Data Breach of security measures required by this Contract that affects the security of any State Data that is subject to applicable Data Breach notification law, the Service Provider shall (1) promptly notify the appropriate State [A12] Identified Contact within 24 [A13] hours or sooner after the Service Provider confirms the Data Breach, unless shorter time is required by applicable law, and unless prior notification is prohibited by court order or other legal requirement, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

6. DATA BREACH RESPONSIBILITIES:

This section only applies when a Data Breach occurs with respect to Personal Data and/or Non-Public Data within the possession or control of a Service Provider and related to service provided under this Contract.

- a. The [A14] Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall immediately notify the appropriate State Identified Contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a Security Incident.
- b. The [A15] Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall promptly notify the appropriate State Identified Contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a Data Breach. The Service Provider shall (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the Data Breach [A16], including conduct any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- c. Service Provider will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service Provider to the State Identified Contact until the Data Breach has been effectively resolved to the State's satisfaction. [A17]
- d. Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair IaaS as needed in accordance with the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.
- e. Unless otherwise stipulated in the SOW and/or SLA, if the Service Provider is required by the Contract to encrypt Personal Data and/or Non-Public Data and a Data Breach is a direct result of the Service Provider's breach of its Contract that obligation, to encrypt Personal Data and/or Non-Public Data otherwise prevent its release, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State (or Federal) law; (4) a website or a toll-free number and call center for affected individuals required by State law; and (5) complete all corrective actions as reasonably determined by the Service Provider based on root cause; all [(1) through (5)] subject to this Contract's Limitation of Liability provision as set forth in the General Provisions – Information Technology.

7. NOTIFICATION OF LEGAL REQUESTS:

STATE MODEL

CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

(Infrastructure as a Service) Amazon

The Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's Data under this Contract, or which in any way might reasonably require access to State's Data. The Service Provider shall not respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, (unless prohibited by law from providing such notice). ~~Service Provider agrees to provide its intended responses to the State [A18] with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction if necessary.~~ Service Provider shall not respond to legal requests directed at the State unless authorized in writing to do so by the State.

8. DATA PRESERVATION AND RETRIEVAL:

- a. For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Service Provider shall ~~make the services available for the State to access State Data, without alteration, for the State to assist the State in extracting and/or transitioning~~ all State Data in the format determined by the State ("Transition Period").[A19]
- b. The Transition Period may be modified in the SOW and/or SLA or as agreed upon in writing by the parties in a Contract amendment.
- c. ~~During [A20] the Transition Period, IaaS and State Data access shall continue to be made available to the State without alteration.~~
- d. Service Provider agrees to compensate the State for ~~damages or losses the State incurs as a result of Service Provider's failure to comply with this section [A21]~~ in accordance with the "Limitation of Liability" provision set forth in the General Provisions - Information Technology.
- e. The State at its option, may purchase additional transition services as agreed upon in the SOW and/or SLA.
- f. During any period of suspension, the Service Provider shall not take any action to intentionally erase any State Data.
- g. ~~The Service Provider will impose no fees for access and retrieval of digital content to the State [A22].~~
- h. After termination of the Contract and the prescribed retention period, ~~the Service Provider shall securely dispose of all State Data in all of its forms, such as disk, CD/ DVD, backup tape and paper [A23]. State Data Infrastructure components shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the State [A24].~~

9. BACKGROUND CHECKS:

As permitted by law, the Service Provider shall conduct criminal background checks and not utilize any staff, including subcontractors, ~~to fulfill the obligations of the Contract [A25] who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty.~~ The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

10. ACCESS TO SECURITY LOGS AND REPORTS:

- a. ~~The Service Provider shall provide reports to the State directly related to the infrastructure the Service Provider controls upon which the State account resides. Unless otherwise agreed to in the SLA, the Service Provider shall provide the State a history of all Application Program Interface (API) calls for the State account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Service Provider. The report will be sufficient to enable the State to perform security analysis, resource change tracking and compliance auditing [A26].~~
- b. The Service Provider and the State recognize that security responsibilities are shared. The Service Provider is responsible for providing a secure infrastructure. The State 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 SOW and/or SLA.

11. CONTRACT AUDIT:

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) Amazon

The Service Provider shall allow the State to audit conformance to the Contract terms. The State may perform this audit or Contract with a third party at its discretion and at the State's expense.

12. DATA CENTER AUDIT:

The Service Provider shall undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit of its data centers at its own expense. The Service Provider shall provide a redacted version[A27] of the audit report ~~and Contractor's plan to correct any negative findings~~ [A28] upon request. The Service Provider may remove its proprietary information from the redacted version.

13. CHANGE CONTROL AND ADVANCE NOTICE:

The Service Provider shall give advance notice (~~as to the extent~~ agreed to by the parties and included in the SOW and/or SLA) to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number[A29].

14. SECURITY PROCESSES:

The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Service Provider[A30]. The State and the Service Provider shall understand each other's roles and responsibilities, which shall be set forth in the SOW and/or SLA.

15. NON-DISCLOSURE AND SEPARATION OF DUTIES:

~~The Service Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, including those that may be required by the State, and limit staff knowledge of State Data to that which is absolutely necessary to perform job duties.~~[A31]

16. IMPORT AND EXPORT OF DATA:

The State shall have the ability to import or export data in whole or in part at its discretion without interference from the Service Provider. This includes the ability for the State to import or export data to or from other Service Providers.

17. RESPONSIBILITIES AND UPTIME GUARANTEE:

The Service Provider 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 environment are the responsibility of the Service Provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), ~~and shall provide service to customers as defined~~ subject to the limitations and any remedies provided for in the SOW and/or SLA.

18. STRATEGIC BUSINESS PARTNER DISCLOSURE:

The Service Provider shall identify all of its strategic business partners related to services provided under this Contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, and who shall be involved in any application development and/or operations[A32].

19. RIGHT TO REMOVE INDIVIDUALS:

The State shall have the right at any time to require the Service Provider remove from interaction with State any Service Provider representative who the State believes is detrimental to its working relationship with the Service Provider. The State shall provide the Service Provider with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) Amazon

violation exists with respect to the request, the Service Provider shall immediately remove such individual. The Service Provider shall not assign the person to any aspect of the Contract or future work orders without the State's consent.

20. **BUSINESS CONTINUITY AND DISASTER RECOVERY:**

The Service Provider shall provide a business continuity and disaster recovery plan upon request and shall ensure that it achieves the State's Recovery Time Objective (RTO), as agreed to by the parties and set forth in the SOW and/or SLA.

- a. ~~In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to State Data, Service Provider shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the Contracting agency. Service Provider shall provide such notification within twenty-four (24) hours after Service Provider reasonably believes there has been such a disaster or catastrophic failure. In the notification, Service Provider shall inform the State of:~~
 - i. ~~The scale and quantity of the State Data loss;~~
 - ii. ~~What Service Provider has done or will do to recover the State Data and mitigate any deleterious effect of the State Data loss; and~~
 - iii. ~~What corrective action Service Provider has taken or will take to prevent future Data loss.~~
 - iv. ~~If Service Provider fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.~~
- b. ~~Service Provider shall restore continuity of IaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair IaaS as needed to meet the performance requirements stated in the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.~~
- e.a. ~~Service Provider shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Service Provider shall cooperate fully with the State, its agents and law enforcement. [A33]~~

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) HPE

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR INFRASTRUCTURE AS A SERVICE (IaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). STATE AGENCIES MUST FIRST:

- A. CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;
- B. CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;
- C. MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.

1. DEFINITIONS:

- a. ~~“Authorized Persons[A1]” means the Service Provider’s employees, Contractors, subcontractors or other agents who need to access the State’s Data to enable the Service Provider to perform the services required.~~
- b.a. “Data Breach” means the confirmed[A2] unauthorized access that results in the use, disclosure, destruction, modification, loss or theft of the State’s unencrypted Personal Data or Non-Public Data.
- c. ~~“Individually Identifiable Health Information[A3]” means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.~~
- d.b. “Infrastructure-as-a-Service” (IaaS) means the capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).
- e.c. “Non-Public Data” means data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, regulation or policy from access by the general public as public information.
- f.d. “Personal Data” means data that includes information relating to a person that identifies the person by name and has any of 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 Hhealth Information (PHI) relating to a person.
- g.e. ~~“Protected Health Information[A4]” (PHI) means the same as the term “Protected Health Information” in 45 C.F.R. 160.103, and shall refer to PHI obtained from Covered Entity or obtained by or created by Business Associate on behalf of Covered Entity. Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.~~ PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.
- h.f. “State Data” means all data created or in any way originating with the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State’s hardware, the Service Provider’s hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Service Provider.
- i.g. “State Identified Contact” means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.

STATE MODEL

CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

(Infrastructure as a Service) HPE

~~j. "Security Incident" [A5] means the potentially unauthorized access to Personal Data or Non-Public Data the Service Provider believes could reasonably result in the use, disclosure or theft of the State's unencrypted Personal Data or Non-Public Data within the possession or control of the Service Provider. A Security Incident may or may not turn into a Data Breach.~~

~~k.h. "Service Level Agreement" (SLA) means a written agreement between both the State and the Service Provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (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) security responsibilities and notice requirements, how disputes are discovered and addressed, and (6) any remedies for performance failures.~~

~~l.i. "Service Provider" means the Contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Contract.~~

~~m.j. "Statement of Work" (SOW) means a written statement in a solicitation document or Contract that describes the State's service needs and expectations.~~

2. **DATA OWNERSHIP:**

The State will own all right, title and interest in State Data that is related to the services provided by this Contract. The State will be the Data Controller of its data at all times and appoints Service Provider as a processor of Personal Data in connection with the Services. [A6] The Service Provider shall not access State user accounts or State 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 Contract, (4) at the State's written request or (5) as required by law.

3. **DATA PROTECTION:**

Protection of personal privacy and data shall be an integral part of the business activities of the Service Provider to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity and availability of State information within its control and comply with the following conditions:

~~a. The Service Provider 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 identified in the Supporting Materials for the particular Service and consistent with the Service Provider's representations concerning the technology environment being provided. The Service Provider is not responsible for viruses or malware introduced by the State or an end user. The State may not use the services in ways that would impose additional regulatory or other legal obligations on the Service Provider unless the parties have expressly agreed to do so in writing. In addition to the Compliance with Statutes and Regulations provisions set forth in the General Provisions – Information Technology~~

~~i. The California Information Practices Act (Civil Code Sections 1798 et seq).~~

~~ii. NIST Special Publication 800-53 Revision 4 or its successor.~~

~~iii. Privacy provisions of the Federal Privacy Act of 1974. [A7]~~

~~b. All State Data obtained by the Service Provider within its control in the performance of this Contract shall become and remain the property of the State. [A8]~~

~~e.a. Unless otherwise stipulated, Personal Data and Non-Public Data shall be encrypted at rest, in use, and in transit with controlled access. The SOW and/or SLA will specify which party is responsible for encryption and access control of the State Data for the service model under Contract. If the SOW and/or SLA and the Contract are silent, then the State is responsible for encryption and access control.~~

~~d.b. Unless otherwise stipulated, it is the State's responsibility to identify data it deems as Non-Public Data to the Service Provider [A9]. The the level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.~~

~~e.c. At no time shall any State data or processes which either belong to or are intended for the use of State or its officers, agents or employees [A10] be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State.~~

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) HPE

4. DATA LOCATION:

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

5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

The Service Provider shall inform the State of any ~~Security Incident or~~ [A11] Data Breach related to State Data within the possession or control of the Service Provider and related to the service provided under this Contract.

~~a. Security Incident Reporting Requirements [A12]: Unless otherwise stipulated, the Service Provider shall immediately report a Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA.~~

~~b.a. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed [A13] Data Breach that affects the security of any State Data that is subject to applicable Data Breach notification law, the Service Provider shall (1) promptly notify the appropriate State Identified Contact within 24 hours or sooner [A14], unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.~~

6. DATA BREACH RESPONSIBILITIES:

This section only applies when a Data Breach occurs with respect to Personal Data and/or Non-Public Data within the possession or control of a Service Provider and related to service provided under this Contract.

~~a. The Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall immediately notify the appropriate State Identified Contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a Security Incident [A15].~~

~~b.a. The Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall promptly notify the appropriate State Identified Contact within 24 hours or sooner [A16] by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that [A17] there has been a Data Breach. The Service Provider shall (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services [A18], if necessary.~~

~~b.b. Service Provider will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service Provider to the State Identified Contact until the Data Breach has been effectively resolved to the State's satisfaction. [A19]~~

~~d. Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair IaaS as needed in accordance with the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract. [A20]~~

~~e.c. Unless otherwise stipulated in the SOW and/or SLA, if a Data Breach is a direct result of the Service Provider's breach of its Contract contractual [A21] obligation to encrypt Personal Data and/or Non-Public Data otherwise prevent its release [A22], the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State (or Federal) law; (4) a website or a toll-free number and call center for affected individuals required by State law; and (5) complete all corrective actions as reasonably determined by the Service Provider based on root cause; all [(1) through (5)] subject to this Contract's Limitation of Liability provision as set forth in the General Provisions – Information Technology.~~

STATE MODEL

CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

(Infrastructure as a Service) HPE

7. NOTIFICATION OF LEGAL REQUESTS:

Unless otherwise required by law, the[A23] The Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's Data under this Contract, or which in any way might reasonably require access to State's Data. The Service Provider shall not respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, unless prohibited by law from providing such notice. Service Provider agrees to provide its intended responses to the State with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. Service Provider shall not respond to legal requests directed at the State unless authorized in writing to do so by the State.

8. DATA PRESERVATION AND RETRIEVAL:

- a. For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Service Provider shall assist the State in extracting and/or transitioning all State Data in the format determined by the State ("Transition Period").
- b. The Transition Period may be modified in the SOW and/or SLA or as agreed upon in writing by the parties in a Contract amendment.
- c. During the Transition Period, IaaS and State Data access shall continue to be made available to the State without alteration as long as the State continues to pay for contracted services. [A24]
- ~~d. Service Provider agrees to compensate the State for damages or losses the State incurs as a result of Service Provider's failure to comply with this section in accordance with the "Limitation of Liability" provision set forth in the General Provisions - Information Technology.~~ [A25]
- ~~e.d.~~ The State at its option, may purchase additional transition services as agreed upon in the SOW and/or SLA.
- ~~f.e.~~ During any period of suspension, the Service Provider shall not take any action to intentionally erase any State Data.
- ~~g.f.~~ The Service Provider will impose no additional [A26] fees for access and retrieval of digital content to the State State Data by the State [A27].
- ~~h.g.~~ After termination of the Contract and the any [A28] prescribed retention period, the Service Provider shall securely dispose of all State Data in all of its forms, such as disk, CD/ DVD, backup tape and paper. State Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the State.

9. BACKGROUND CHECKS:

As permitted by law, the Service Provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty within the past five years. [A29] The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

10. ACCESS TO SECURITY LOGS AND REPORTS:

- a. As described in the SOW or SLA, the [A30] The Service Provider shall provide reports to the State directly related to the infrastructure the Service Provider controls upon which the State account resides. Unless otherwise agreed to in the SLA and to the extent available as part of the services [A31], the Service Provider shall provide the State a history of all Application Program Interface (API) calls for the State account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Service Provider. The report will be sufficient to enable the State to perform security analysis, resource change tracking and compliance auditing.

STATE MODEL

CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

(Infrastructure as a Service) HPE

- b. The Service Provider and the State recognize that security responsibilities are shared. The Service Provider is responsible for providing a secure infrastructure. The State 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 SOW and/or SLA.

11. CONTRACT AUDIT:

The Service Provider shall allow the State reasonable access [A32] to audit conformance to the Contract terms no more than once annually [A33]. The State may perform this audit or Contract with a third party at its discretion and at the State's expense. In no event will Service Provider be required to provide the State or its auditor with access to Service Provider's internal costs and resource utilization data, or data related to employees or other customers of Service Provider. [A34]

12. DATA CENTER AUDIT:

The Service Provider shall undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit of its data centers at its own expense. The Service Provider shall provide a redacted version of the audit report and Contractor's plan to correct any negative findings upon request. The Service Provider may remove its proprietary information from the redacted version.

13. CHANGE CONTROL AND ADVANCE NOTICE:

The Service Provider shall give advance notice (as agreed to by the parties and included in the SOW and/or SLA) to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number. Service Provider may change the features and functionality of the services, without degrading them, to make improvements, address security requirements and comply with changes in law. In the event a Service Provider change eliminates or reduces any services or Service Levels, Service Provider will provide the State with at least 18 months' advanced notice [A35] and the State may terminate the services with 30 days written notice and without paying a termination charge.

14. SECURITY PROCESSES:

The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Service Provider. The State and the Service Provider shall understand each other's roles and responsibilities, which shall be set forth in the SOW and/or SLA.

15. NON-DISCLOSURE AND SEPARATION OF DUTIES:

The Service Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, including those that may be required by the State, [A36] and limit staff knowledge of State Data to that which is absolutely [A37] necessary to perform job duties.

16. IMPORT AND EXPORT OF DATA:

The State shall have the ability to import or export data in whole or in part at its discretion without interference from the Service Provider. This includes the ability for the State to import or export data to or from other Service Providers.

17. RESPONSIBILITIES AND UPTIME GUARANTEE:

The Service Provider 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 environment are the responsibility of the Service Provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and shall provide service to customers as defined in the SOW and/or SLA.

18. STRATEGIC BUSINESS PARTNER DISCLOSURE:

STATE MODEL

CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

(Infrastructure as a Service) HPE

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

19. RIGHT TO REMOVE INDIVIDUALS:

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

20. BUSINESS CONTINUITY AND DISASTER RECOVERY:

To the extent available as part of the services, the T[A38]he Service Provider shall provide a business continuity and disaster recovery plan upon request and shall ensure that it achieves the State's Recovery Time Objective (RTO), as agreed to by the parties and set forth in the SOW and/or SLA.

- a. In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to State Data, Service Provider shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the Contracting agency. Service Provider shall provide such notification within twenty-four (24) hours after Service Provider reasonably believes there has been such a disaster or catastrophic failure. In the notification, to the extent possible[A39], Service Provider shall inform the State of:
 - i. The scale and quantity of the State Data loss;
 - ii. What Service Provider has done or will do to recover the State Data and mitigate any deleterious effect of the State Data loss; and
 - iii. What corrective action Service Provider has taken or will take to prevent future Data loss.
 - ~~iv. If Service Provider fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract[A40].~~
- b. Service Provider shall restore continuity of IaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair IaaS as needed to meet the performance requirements stated in the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract[A41].
- c. Service Provider shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Service Provider shall cooperate fully with the State, its agents and law enforcement.

21. LIMITED USE[A42]:

Products and services provided under these terms are for the State's internal use and not for further commercialization. The State is responsible for complying with applicable laws and regulations, including but not limited to, obtaining any required export or import authorizations if the State exports, imports or otherwise transfers products or deliverables provided under Contract.

22. ORDERING[A43]:

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) HPE

“Order” means the accepted order including any supporting materials which the parties identify as incorporated either by attachment or reference (“Supporting Materials”). Supporting Materials may include (as examples) product lists, hardware or software specifications, standard or negotiated service descriptions, data sheets and their supplements, supplementary terms, policies, and statements of work (SOWs), published warranties and service level agreements, and may be available to the State in hard copy or by accessing a designated Service Provider website.

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

d. The Service Provider shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the State.

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

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

(1) The services description 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 State representative;

(5) The price per unit or other pricing elements consistent with this Contract and the Service Provider’s proposal;

(6) A ceiling amount of the order for services being ordered; and

(7) The Contract identifier;

(8) The Security Features, if any;

(9) The Acceptable Use Policy (as updated from time to time); and

(10) The Notification Policy (as updated from time to time).

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

h. Orders must be placed pursuant to this Contract before the termination date of this Contract. Service Provider is reminded that financial obligations of the State 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 Contract, Service Provider agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Service Provider shall not honor any Orders placed after the expiration or termination of this Contract. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Contract may not be placed after the expiration or termination of this Contract, notwithstanding the term of any such indefinite delivery order agreement.

23. TITLE TO PRODUCT^[A44]:

If access to the services requires an application program interface (API), Service Provider shall convey to the State an irrevocable and perpetual license to use the API. No transfer of ownership of any intellectual property will occur under this Contract. The State grants Service Provider a non-exclusive, worldwide, royalty-free right and license to any intellectual property that is necessary for the Service Provider and its designees to perform the ordered services. If deliverables are created by Service Provider specifically for the State and identified as such in Ordering materials, the Service Provider grants the State a worldwide, non-exclusive, fully paid, royalty-free license to reproduce and use copies of the deliverables internally.

24. SUSPENSION OF SERVICES^[A45]:

Service Provider may suspend provision of services to the State in the following limited circumstances: (i) Service Provider reasonably believes the services are, have been, or will be used in violation of the Contract; (ii) Service Provider reasonably believes suspension is necessary to protect Service Provider’s network, systems, operations or other users; or (iii) suspension is required by law. If Service

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) HPE

Provider suspends the services, the parties will cooperate to identify and rectify any issues so that services may be restored as soon as reasonably possible.

25. CHANGE ORDERS^[A46]:

State's requests to change the scope of services or products, on a per-Order basis, will require a change order signed by the State and the Service Provider.

26. EUROPEAN PERSONAL DATA^[A47]:

If the State reasonably anticipates or discovers that its use of the services will involve storage or processing of Personal Data from the European Economic Area ("EEA") or Switzerland, the State will inform Service Provider, and provide whatever information Service Provider reasonably requests related to that storage or processing. Upon the State's request, Service Provider will enter into (or cause its Affiliates to enter into) EU Model Contract(s) with appendices (including technical and organizational security measures) in the form from time to time used by the Service Provider and its Affiliates (and available to the State upon request). The State appoints Service Provider as its agent to execute EU Model Contracts on the State's behalf.

27. GLOBAL TRADE COMPLIANCE^[A48]:

Imports, exports and other transfers of data or software stored, used or processed using the services or related infrastructure are the State's sole responsibility, and the State will obtain any authorizations that may be required. The State will not use, distribute, transfer, or transmit any products, software or technical information (even if incorporated into other products) in violation of applicable export laws and regulations. In particular, the State, and any third party authorized by the State, may not, in violation of applicable laws and regulations, transfer, or authorize the transfer, of any services into U.S. embargoed countries or to anyone on the U.S. Treasury Department's List of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders or Entity List of proliferation concern, or the U.S. State Department's Debarred Parties List.

STATE MODEL
CLOUD COMPUTING SERVICES SPECIAL PROVISIONS
(Infrastructure as a Service)
IBM's Comments

IaaS Special Provisions Section No.	IBM's Comments
Introduction and general comments	<p>IBM IaaS is meant to be a self-managed service and the features that are activated depend on the options selected by the customer. Many features described in these terms are activated only if the customer selects the feature. Some are available at an extra cost. These Special Provisions need to reflect the flexibility are contemplated by IaaS. Because of the unmanaged nature of IaaS, IBM cannot commit to all the terms and conditions in this document for all IaaS offered by IBM. For example:</p> <p>SOFTLAYER (self-managed)</p> <p>Cloud Managed Services IaaS has Options for High Availability, PCI, HIPAA, DR, Migration Services,</p> <p>zOS includes a Private Cloud Mainframe</p> <p>Additionally, similar to the SaaS Special Provision, contractors should have the ability to modify the IaaS Special Provisions in a SOW.</p>
1. Definitions	<p>“Authorized Users” - For IaaS, not all the individuals identified in the definition of “Authorized Users” will have full access to IaaS. Generally, there is a Client Account Administrator – responsible for authorized State actions to administer the environment</p>
	<p>“State Data” – IBM uses the term “Content” which is broader than the State’s definition of “State Data”. IBM suggests that the State consider this broader definitions of “Content” in place of “State Data”: all data, software, solutions, products, prototypes technical data and information, including, without limitation, any hypertext markup language files, scripts, programs, recordings, sound, music, graphics, images, applets, or servlets that are created, installed, uploaded, or transferred in connection with the Services by the State, users, or solution recipients</p>
	<p>“Security Incident” – Delete “potentially”. IaaS is not set up to notify</p>

	customers of “potential” issues. IBM provides notice when it becomes aware of unauthorized access, not necessarily a potential situation.
	“Service Level Agreement” – Default SLA terms should not apply. SLAs should apply only if part of a Services Description. Dispute resolution is not included in the SLA but could be included in a SOW.
3. Data Protection	<p>For IaaS, safeguarding the confidentiality, integrity and availability of State information is subject to the State’s control, not the Contractor’s control. The State implements the controls that are available to it as features of IaaS.</p> <p>a.1 should read “The California Information Practices Act (Civil Code Sections 1798 et seq) applicable to Service Provider as a provider of IaaS”</p> <p>a.2 should read: “Service Provider provides physical security measures for computing environments hosting Cloud Services in accordance with the NIST 800-53 framework.”</p> <p>a.3 should read: “Privacy provisions of the Federal Privacy Act of 1974 applicable to Service Provider as a provider of IaaS and only to the extent required by a U.S. governmental agency for this scope of services.”</p> <p>3.c Encryption available in IaaS is the responsibility of the State. The user of IaaS is responsible for encryption and access control.</p> <p>3.d Customers will be informed of encryption levels and options, but this generally would not be part of the contract.</p>
4. Data Location	Data centers are located globally. However, if the State wants to use data centers located only in the US, it is the State’s responsibility to designate data center locations and the State has control over where data resides or is transferred.
5. Security Incident	<p>Entire Section 5: Flexibility is required. This section should be preceded with “Unless otherwise described in a Service Description or Statement of Work...”</p> <p>5.a Most of IaaS offerings are unmanaged services, meaning these are managed by the customer, not the Service Provider. IBM can agree to provide notification of Security Incidents of which it is aware, but the State, in an unmanaged environment, may become aware of a Security Incident before Service Provider is, in which case the State should notify Service Provider.</p> <p>“Immediately” is too stringent. Service Provider needs sufficient time</p>

	<p>(whether a few hours or several days) to gather facts and determine an incident occurred. Since the State may be aware of an incident first, it is suggest that a more balanced approach be adopted: “In the event either party becomes aware of a Security Incident, such party will promptly (and no more than required under applicable law, to the extent that any such law applies to notifications between a supplier and Box) notify the other party of such Security Incident in writing...” Additionally, notices of Security Incidents go out to all IaaS customers at the same time. We cannot accommodate a different notice schedule for individual customers.</p> <p>5.b See comments above for 5.b. Not all measures may apply to PaaS. Flexibility is required to adapt these terms to the particular offering.</p>
<p>6. Data Breach Responsibilities</p>	<p>IaaS is managed, so Service Provider does not possess the Content nor control the environment in which it is contained. IBM suggests a more balanced approach for reasons stated above:</p> <p>“In case either party reasonably suspects any loss of, unauthorized access to or unauthorized disclosure of Box Content (each a “Security Incident”), such party will promptly (and no more than required under applicable law, to the extent that any such law applies to notifications between a Service Provider and State) notify the other party of such Security Incident in writing (e.g., via email) upon becoming aware thereof and provide sufficient details to enable Service Provider to identify the (suspected) breach and the notified party will provide reasonable assistance to conduct a review of the same.</p> <p>Notice will be made to the mechanisms established for this account. IBM will use standard notification mechanisms as managed by State. State will notify Service Provider through standard mechanisms including but not limited to creating a “Security Issue” Service Ticket or notification to the State assigned Technical Account Manager.</p> <p>The notified party must cooperate fully with the notifying party’s reasonable requests for information regarding the Security Incident, and must provide regular updates on each Security Incident and the investigative action and corrective action taken as required.</p>
<p>8. Data Preservation and Retrieval</p>	<p>Under the self-managed approach the State migrates data in and is responsible to migrate out. If State requires assistance from Service Provider, such assistance must be contracted for as additional migration /managed services. Format may vary depending upon offering. IBM may charge for certain transition activities such as delivering content in a specific format.</p> <p>a.b. and c. need to be modified to reflect the above requirements.</p>

9. Background Checks	<p>Replace 9 with:</p> <p>When required under a Statement of Work, and at the State’s expense, the Service Provider shall conduct a background investigation in accordance with Service Provider’s internal process. These inquiries will include felony/misdemeanor criminal court searched based on all addresses associated with the last seven (7) years of the individual’s resident history, including convictions and pending charges. The background report will also include a check of a national criminal database as well as the OFAC Listing. Service Provider’s personnel acquired through acquisition may or may not have been screened with recent background checks.</p>
10. Access to Security Logs and Reports	<p>This section is not entirely accurate. IaaS provides State with the ability to “self-manage”, meaning create, monitor and store logs by itself. A Cloud Manage Service Delivery model provides limited reference to security logs. Depending upon Service Options chosen for i.e. HIPAA, PCI, etc. may have enhanced capability to create, monitor and store logs. This must be addressed in a SOW.</p>
12. Data Center Audit	<p>Section 12 needs additional details and clarification. IBM recommends the following:</p> <p>Service Provider will arrange for the performance of audits and production of an audit report by an independent third party in accordance with the most recent “Service Organizational Control Type II Report” made in accordance with Statements on Standards for Attestation Engagements No. 16 (“SOC2 Report”) covering the computing environments used to host Cloud Services. Service Provider will provide a single SOC2 Report covering all computing environment locations hosting Cloud Services. Each SOC2 Report will include an audit of the security, availability and confidentiality of the controls in place for the computing environment and data center physical facilities. An independent third party auditor issues such SOC2 Report at least annually covering operations since the prior SOC2 Report.</p>
13. Change Control and Advance Notice	<p>This depends on the service and must be mutually agreed in a SOW.</p>
14. Security Processes	<p>Delete or further discuss this provision. It is unclear to IBM as to what the State considers as the Service Provider’s non-proprietary security processes and technical limitations.</p>

15. Non-Disclosure and Separation of Duties	This provision is unclear. More information regarding the intent is requested.
19. Right to Remove Individuals ¹	Delete as these are individuals that are supporting multiple IaaS accounts and individuals may be critical to support. A better approach would be for the State to raise concerns to Service Provider to address and discuss appropriate measures with the State.
20. Business Continuity and Disaster Recovery	This section should be deleted or should reference the capabilities that are predefined in the product. For IaaS, these services are not customized for individual customers. It is the state's responsibility to determine whether the predefined RTO meets their requirements.
General Provisions - IT: 16. Inspection, Acceptance and Rejection	Inspection, Acceptance and Rejection does not apply to IaaS. Once the customer purchases IaaS, the service begins. There is no ability to reject the service, other than as part of the termination provisions that accompany the service.
General Provisions – IT: 26. Limitation of Liability	Limitation of Liability – Commercially standard limitation is 12 months charges. This should be the limitation on direct damages rather than 1x Purchase Price (which could be for more than one year).
General Provisions – IT: 46. Examination and Audit	The records that will be made available to the State will only be those that document the State's usage of the IaaS. Records relating to multi-tenant usage will not be made available, due to confidentiality concerns.

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) SHI

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR INFRASTRUCTURE AS A SERVICE (IaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). STATE AGENCIES MUST FIRST:

- A. CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;
- B. CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;
- C. MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.

1. DEFINITIONS:

- a. "Authorized Persons" means the Service Provider's employees, Contractors, subcontractors or other agents who need to access the State's Data to enable the Service Provider to perform the services required.
- b. "Data Breach" means the unauthorized access that results in the use, disclosure, destruction, modification, loss or theft of the State's unencrypted Personal Data or Non-Public Data.
- c. "Individually Identifiable Health Information" means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- d. "Infrastructure-as-a-Service" (IaaS) means the capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).
- e. "Non-Public Data" means data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, regulation or policy from access by the general public as public information.
- f. "Personal Data" means data that includes information relating to a person that identifies the person by name and has any of 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.
- g. "Protected Health Information" (PHI) means Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.
- h. "State Data" means all data created or in any way originating with the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, the Service Provider's hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Service Provider.
- i. "State Identified Contact" means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.
- j. "Security Incident" means the potentially unauthorized access to Personal Data or Non-Public Data the Service Provider believes could reasonably result in the use, disclosure or theft of the State's unencrypted Personal Data or Non-Public Data within the possession or control of the Service Provider. A Security Incident may or may not turn into a Data Breach.

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) SHI

- k. "Service Level Agreement" (SLA) means a written agreement between both the State and the Service Provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (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) security responsibilities and notice requirements, how disputes are discovered and addressed, and (6) any remedies for performance failures.
- l. "Service Provider"^[NS1] means either: (i) the Contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Contract; or (ii) if the Contractor is not the service provider, the third party contracted with Contractor to provide the IaaS services under this Contract.
- m. "Statement of Work" (SOW) means a written statement in a solicitation document or Contract that describes the State's service needs and expectations.

2. DATA OWNERSHIP:

The State will own all right, title and interest in State Data that is related to the services provided by this Contract. The Contractor shall not, and ensure the Service Provider shall not, access State user accounts or State 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 Contract, (4) at the State's written request or (5) as required by law.

3. DATA PROTECTION:

Protection of personal privacy and data shall be an integral part of the business activities of the Contractor and Service Provider to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Contractor shall ensure the Service Provider shall safeguards the confidentiality, integrity and availability of State information within its control and comply with the following conditions:

- a. In addition to the Compliance with Statutes and Regulations provisions set forth in the General Provisions – Information Technology
 - i. The California Information Practices Act (Civil Code Sections 1798 et seq).
 - ii. NIST Special Publication 800-53 Revision 4 or its successor.
 - iii. Privacy provisions of the Federal Privacy Act of 1974.
- b. All State Data obtained by the Contractor and/or Service Provider within its control in the performance of this Contract shall become and remain the property of the State.
- c. Unless otherwise stipulated, Personal Data and Non-Public Data shall be encrypted at rest, in use, and in transit with controlled access. The SOW and/or SLA will specify which party is responsible for encryption and access control of the State Data for the service model under Contract. If the SOW and/or SLA and the Contract are silent, then the State is responsible for encryption and access control.
- d. Unless otherwise stipulated, it is the State's responsibility to identify data it deems as Non-Public Data to the Service Provider. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.
- e. At no time shall any data or processes — which either belong to or are intended for the use of State or its officers, agents or employees — be copied, disclosed or retained by the Contractor or Service Provider or any party related to the Contractor or Service Provider for subsequent use in any transaction without the express written consent of the State.

4. DATA LOCATION:

The Contractor shall ensure the Service Provider shall provides its services to the State and its end users solely from data centers in the continental United States^[NS2]. Storage of State Data at rest shall be located solely in data centers in the continental United States. The Contractor shall ensure the Service Provider shall does not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor Service Provider shall permit its personnel, and contractors and Service Provider to access State Data remotely only as

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) SHI

required to provide technical or customer^[NS3] support. ~~T~~The Service Provider may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this Contract or provided in an SOW^[NS4].

5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

The Contractor shall ensure the Service Provider shall inform~~s~~ the State of any Security Incident or Data Breach related to State Data within the possession or control of the Service Provider and related to the service provided under this Contract.

- a. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall ensure the Service Provider shall immediately report~~s~~ a Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA.
- b. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed Data Breach that affects the security of any State Data that is subject to applicable Data Breach notification law, the Contractor shall ensure Service Provider shall (1) promptly notifi~~es~~y the appropriate State Identified Contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take~~s~~ commercially reasonable measures to address the Data Breach in a timely manner.

6. DATA BREACH RESPONSIBILITIES:

This section only applies when a Data Breach occurs with respect to Personal Data and/or Non-Public Data within the possession or control of a Service Provider and related to service provided under this Contract.

- a. The Contractor shall ensure the Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall immediately notifi~~es~~y the appropriate State Identified Contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a Security Incident.
- b. The Contractor shall ensure the Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall promptly notifi~~es~~y the appropriate State Identified Contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a Data Breach. The Contractor shall ensure the Service Provider shall (1) cooperate~~s~~ with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement~~s~~ necessary remedial measures, if necessary; and (3) document~~s~~ responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- c. The Contractor shall ensure Service Provider will provide~~s~~ daily-weekly updates, or more frequently if required by the State agreed to by the parties, regarding findings and actions performed by Service Provider to the State Identified Contact until the Data Breach has been effectively resolved to the State's satisfaction.
- d. The Contractor shall ensure the Service Provider shall quarantine~~s~~ the Data Breach, ensure~~s~~ secure access to Data, and repair~~s~~ IaaS as needed in accordance with the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.
- e. Unless otherwise stipulated in the SOW and/or SLA, if a Data Breach is a direct result of the Service Provider's breach of its Contract obligation to encrypt Personal Data and/or Non-Public Data or^[NS5] otherwise prevent its release, the ~~Service Provider~~Contractor shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State (or Federal) law; (4) a website or a toll-free number and call center for affected individuals required by State law; and (5) complete all corrective actions as reasonably determined by the Contractor and/or Service Provider based on root cause; all [(1) through (5)] subject to this Contract's Limitation of Liability provision as set forth in the General Provisions – Information Technology.

7. NOTIFICATION OF LEGAL REQUESTS:

The Contractor shall, or ensure the Service Provider shall, contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's Data under this Contract, or which in any way might reasonably

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) SHI

require access to State's Data. ~~Neither the Contractor nor the~~ Service Provider shall ~~not~~ respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, unless prohibited by law from providing such notice. The Contractor shall, and ensure the Service Provider shall, agrees to provide its intended responses to the State with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. Neither the Contractor nor the Service Provider shall ~~not~~ respond to legal requests directed at the State unless authorized in writing to do so by the State.

8. DATA PRESERVATION AND RETRIEVAL:

- a. ~~For ninety (90) days~~^[NS6] prior to the expiration date of this Contract, or upon notice of termination of this Contract, Contractor shall ensure the Service Provider ~~shall assist~~ the State in extracting and/or transitioning all State Data in the format determined by the State ("Transition Period").
- b. The Transition Period may be modified in the SOW and/or SLA or as agreed upon in writing by the parties in a Contract amendment.
- c. During the Transition Period, IaaS and State Data access shall continue to be made available to the State without alteration.
- d. ~~Service Provider~~The Contractor agrees to compensate the State for damages or losses the State incurs as a result of Service Provider's failure to comply with this section in accordance with the "Limitation of Liability" provision set forth in the General Provisions - Information Technology.
- e. The State at its option, may purchase additional transition services as agreed upon in the SOW and/or SLA.
- f. During any period of suspension, the Contractor shall, and ensure the Service Provider shall not take any action to intentionally erase any State Data.
- g. The ~~Service Provider~~Contractor will impose no fees for access and retrieval of digital content to the State.
- h. After termination of the Contract and the prescribed retention period, the Contractor shall, and ensure the Service Provider shall securely dispose of all State Data in all of its tangible forms, such as disk, CD/ DVD, ~~backup tape~~^[NS7] and paper. State Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the State.

9. BACKGROUND CHECKS:

As^[NS8] permitted by law, the Contractor shall ensure the Service Provider ~~shall conduct~~ criminal background checks and not utilize any staff, including subcontractors, to fulfill the ~~obligations of the Contract~~services who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall, and ensure the Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the ~~Service Provider's~~their respective employees and agents.

10. ACCESS TO SECURITY LOGS AND REPORTS:

- a. The Contractor shall ensure the Service Provider ~~shall provide~~ reports to the State directly related to the infrastructure the Service Provider controls upon which the State account resides. Unless otherwise agreed to in the SLA, the Contractor shall ensure the Service Provider ~~shall provide~~ the State a history of all Application Program Interface (API) calls for the State account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Service Provider. The report will be sufficient to enable the State to perform security analysis, resource change tracking and compliance auditing.
- b. The ~~Service Provider~~Contractor and the State recognize that security responsibilities are shared. The Contractor is responsible for ensuring the Service Provider ~~is responsible for providing~~provides a secure infrastructure. The State is responsible for its secure

STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Infrastructure as a Service) SHI

guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SOW and/or SLA.

11. CONTRACT AUDIT:

The ~~Service Provider~~Contractor shall allow the State to audit ~~Contractor's and Service Provider's~~ conformance to the Contract terms, provided the parties first agree to the scope, timing, duration and expectations of the audit.[NS9] The State may perform this audit or Contract with a third party at its discretion and at the State's expense.

12. DATA CENTER AUDIT:

The Contractor shall ensure the Service Provider[NS10] shall undergoes an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit of its data centers at ~~its own expense~~no cost to the State. The ~~Contractor Service Provider~~ shall provide a redacted version of the Service Provider's audit report and ~~Contractor's~~its plan to correct any negative findings upon request. The Service Provider may remove its proprietary information from the redacted version.

13. CHANGE CONTROL AND ADVANCE NOTICE:

The Contractor shall ensure the Service Provider[NS11] shall gives advance notice (as agreed to by the parties and included in the SOW and/or SLA) to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware ware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

14. SECURITY PROCESSES:

The Contractor shall, and ensure the Service Provider shall, disclose its their respective non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Contractor and Service Provider, as applicable. The State and the ~~Service Provider~~Contractor shall understand each other's, and the Service Provider's, roles and responsibilities, which shall be set forth in the SOW and/or SLA.

15. NON-DISCLOSURE AND SEPARATION OF DUTIES:

The ~~Service Provider~~Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, including those that may be required by the State, and limit staff knowledge of State Data to that which is absolutely necessary to perform job duties.

16. IMPORT AND EXPORT OF DATA:

The State[NS12] shall have the ability to import or export data in whole or in part at its discretion without interference from the Contractor and/or Service Provider. This includes the ability for the State to import or export data to or from other Service Providers.

17. RESPONSIBILITIES AND UPTIME GUARANTEE:

The ~~Service Provider~~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 environment are the responsibility of the Service Provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and shall provide service to customers as defined in the SOW and/or SLA.

18. STRATEGIC BUSINESS PARTNER DISCLOSURE:

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

19. RIGHT TO REMOVE INDIVIDUALS:

STATE MODEL

CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

(Infrastructure as a Service) SHI

The State shall have the right at any time to ~~require request [NS13]~~ the ~~Service Provider~~ Contractor remove from interaction with State any ~~Contractor or~~ Service Provider representative who the State believes is detrimental to its working relationship with the ~~Service Provider~~ Contractor. The State shall provide the ~~Contractor~~ Service Provider with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, and if the Contractor determines in its reasonable discretion that the potential violation is valid, the ~~Service Provider~~ Contractor shall immediately remove such individual. The ~~Service Provider~~ Contractor shall not assign the person to any aspect of the Contract or future work orders without the State's consent.

20. **BUSINESS CONTINUITY AND DISASTER RECOVERY:** [NS14]

The Contractor shall ensure the Service Provider ~~shall~~ provides a business continuity and disaster recovery plan upon request and shall ensure that it achieves the State's Recovery Time Objective (RTO), as agreed to by the parties and set forth in the SOW and/or SLA.

- a. In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to State Data, the Contractor shall ensure the Service Provider ~~shall~~ notifies the State by the fastest means[NS15] available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the Contracting agency. The Contractor shall ensure the Service Provider ~~shall~~ provides such notification within twenty-four (24) hours after Service Provider reasonably believes there has been such a disaster or catastrophic failure. In the notification, the Contractor shall ensure the Service Provider ~~shall~~ informs the State of:
 - i. The scale and quantity of the State Data loss;
 - ii. What Service Provider has done or will do to recover the State Data and mitigate any deleterious effect of the State Data loss; and
 - iii. What corrective action Service Provider has taken or will take to prevent future Data loss.
 - iv. If Service Provider fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.
- b. The Contractor shall ensure the Service Provider ~~shall~~ restores continuity of IaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair IaaS as needed to meet the performance requirements stated in the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.
- c. The Contractor shall ensure the Service Provider ~~shall~~ conducts an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. The Contractor shall ensure the Service Provider ~~shall~~ cooperates fully with the State, its agents and law enforcement.