

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR PLATFORM AS A SERVICE (PaaS), 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. “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.
- e.c. “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.
- f.d. “Platform-as-a-Service” (PaaS) means 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.
- 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 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.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

### (Platform as a Service)

~~j. "Security Incident"<sup>[A5]</sup> 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.i. "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 <sup>[A6]</sup> 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. 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:

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.

~~a. In addition to the Compliance<sup>[A7]</sup> 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 Service Provider within its control in the performance of this Contract shall become and remain the property of the State.<sup>[A8]</sup>~~

~~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. Encryption of Data at Rest: Where provided as part of the services, the<sup>[A9]</sup> The Service Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data and Non-Public Data unless otherwise approved by the State,<sup>[A10]</sup> unless the Service Provider presents a justifiable~~

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

~~position approved by the State that Personal Data and Non-Public Data must be stored on a Service Provider portable device in order to accomplish work as defined in the SOW and/or SLA.~~

~~e.c. Unless otherwise stipulated, it is the State's responsibility to identify data it deems as Non-Public Data to the Service Provider. [A11]  
The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.~~

~~f.d. At no time shall any State data or processes — which either belong to or are intended for the use of State [A12] — 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 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 [A13] or~~ Data Breach within the possession and control of the Service Provider and related to service provided under this Contract.

~~a. Incident Response [A14]: The Service Provider may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing Security Incidents with the State should be handled on an urgent as-needed basis, as part of Service Provider communication and mitigation processes as mutually agreed, defined by law or contained in the Contract.~~

~~b. —~~

~~c. Security Incident Reporting Requirement [A15]: 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.~~

~~d.a. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed [A16] Data Breach that affects the security of any State content 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 [A17], 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 [A18].~~

~~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 [A19] or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there [A20] 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 [A21], if necessary.~~

# STATE MODEL

## CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

### (Platform as a Service)

~~e. Service Provider will provide daily updates [A22], 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.~~

~~d.b. Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair PaaS 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. [A23]~~

~~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 [A24] obligation to encrypt Personal Data and/or Non-Public Data, otherwise prevent its release [A25], 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:**

~~Unless otherwise required by law [A26], the~~ 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, PaaS and State Data access shall continue to be made available to the State without alteration as long as the State continues to pay for the contracted services [A27].

~~d. Service Provider agrees [A28] 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.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 [A29] fees for access and retrieval of digital content to the State State Data by the State [A30].~~

~~h.g. After termination of the Contract and any the [A31] 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,

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

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[A32]. 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[A33], ~~the~~The Service Provider shall provide reports to the State in a format as specified in the SOW and/or SLA and agreed to by both the Service Provider and the State. To the extent this information is available [A34]as part of the services, Reports will include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this Contract.
- 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 [A35] to audit conformance to the Contract terms no more than once annual[A36]. 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[A37].

## 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[A38] 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[A39] non-disclosure agreements, including those that may be required by the State, and limit staff knowledge of State Data to that which is absolutely[A40] necessary to perform job duties.

## 16. IMPORT AND EXPORT OF DATA:

# STATE MODEL

## CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

### (Platform as a Service)

---

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:

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~~<sup>A41</sup>~~e services, 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, ~~to the extent possible~~<sup>A42</sup>, 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 resp~~<sup>A43</sup>~~ond 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 PaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair PaaS as needed to meet the performance requirements stated in the SOW and/or SLA. ~~Failure to do so~~<sup>A44</sup>~~may result in the State exercising its options for assessing damages or other remedies under this Contract.~~
- 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. COMPLIANCE WITH ACCESSIBILITY STANDARDS:

The Service Provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

## 22. WEB SERVICES:

The Service Provider shall use Web services exclusively [A45] to interface with State Data in near real time when possible.

## 23. LIMITED USE [A46]:

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.

## 24. ORDERING [A47]:

"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.

## 25. TITLE TO PRODUCT [A48]:

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

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.

## **26. SUSPENSION OF SERVICES**<sup>[A49]</sup>:

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 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.

## **27. CHANGE ORDERS**<sup>[A50]</sup>:

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.

## **28. EUROPEAN PERSONAL DATA**<sup>[A51]</sup>:

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.

## **29. GLOBAL TRADE COMPLIANCE**<sup>[A52]</sup>:

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**  
**(Platform as a Service)**  
**IBM's Comments**

---

PaaS Special Provisions Section No.	IBM's Comments
Introduction and general comments	<p>IBM PaaS provides the use of a shared infrastructure across multiple customers with each individual customer's applications located on their virtual hardware resources and operating systems based upon selected usage entitlements. 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 PaaS. Because of the numerous applications supported and managed under PaaS offerings, IBM cannot commit to all the terms and conditions in this document for all PaaS offered by IBM. For example:</p> <p>Analytics as a Service,</p> <p>Bluemix Development and Test,</p> <p>Cloud Managed Services for Oracle and SAP</p> <p>have numerous options and levels of support for standard, enhanced and premium builds, development and production environments, network connections, DR, and Migration Services.</p> <p>Additionally, similar to the SaaS Special Provision, contractors should have the ability to modify the PaaS Special Provisions in a SOW.</p>
1. Definitions	<p>"Authorized Users" - For PaaS, not all the individuals identified in the definition of "Authorized Users" will have full access to PaaS. Generally, there is a Client Account Administrator/Client Business Point of Contact – 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,</p>

	images, applets, or servlets that are created, installed, uploaded, or transferred in connection with the Services by the State, users, or solution recipients
	“Security Incident” – Delete “potentially”. PaaS is not set up to notify 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 selected. Dispute resolution is not included in the SLA but could be included in a SOW.
3. Data Protection	<p>For PaaS, 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 PaaS selected.</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 PaaS”</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 PaaS and only to the extent required by a U.S. governmental agency for this scope of services.”</p> <p>3.c Encryption options available among PaaS vary. The user of PaaS is responsible to determine type(s) of encryption and extent of 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 Incident response communication procedures are addressed in selected PaaS offerings, and their security controls and security policy</p>

	<p>management documents.</p> <p>5.b Most of PaaS offerings are managed services support up to operating system and underlying infrastructure, with various options available for application and database layers managed by the customer, Service Provider, or jointly shared. IBM can agree to provide notification of Security Incidents of which it is aware, but within the control of State’s managed portion of the 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 (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 PaaS customers at the same time. We cannot accommodate a different notice schedule for individual customers.</p> <p>5.c 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>PAAS is managed, so Service Provider does not possess the Content nor control the application or database 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 “<b>Security Incident</b>”), 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/IBM Point</p>

	<p>of Contact.</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>Generally under the PaaS managed approach the State migrates data in, manages data during steady state 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. Flexibility is needed to be modify these sections to adapt them to a particular offering.</p>
<p>9. Background Checks</p>	<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>
<p>10. Access to Security Logs and Reports</p>	<p>This section is not entirely accurate. PaaS provides State standardized processes and reports as identified in SOW with regard to the IBM controlled and managed environment administering the creation, monitoring and storage of logs under its control. A Cloud Manage Service Delivery model provides limited reference to security logs. Depending upon Service Options chosen may have enhanced capability to create, monitor and store logs. This must be addressed in a SOW.</p>
<p>12. Data Center Audit</p>	<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</p>

	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.
13. Change Control and Advance Notice	This depends on the service and must be mutually agreed in a SOW.
14. Security Processes	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.
15. Non-Disclosure and Separation of Duties	This provision is unclear. More information regarding the intent is requested.
19. Right to Remove Individuals	Delete as these are individuals that are supporting multiple PaaS 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 standard products. For PaaS, these services are not customized for individual customers but provide a number of standard options available for specific applications disaster recovery. It is the state’s responsibility to determine whether the predefined RTO options available meets their requirements. Alternatively, customized Business Continuity and Disaster Recovery services may provided under a separate SOW.
21. Compliance with Accessibility Standards	Contractors should be required to comply with the Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 only to the extent the law actually applies, i.e, when the service is provided to the Federal government of agency. The General Provisions – IT, Section 7, already require Contractors to comply with applicable statutes, rules, regulations and orders of the United States and the State of California. This Section 21 should not be necessary.
22. Web Services	“The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible.” We generally agree that Web services will interface with State Data in near real time when possible. However, there may be situations where we mutually agree to use physical direct tape/hardware to transfer large volumes of data

	to and from web environment instead of over internet would be time prohibitive and impractical. We suggest adding “or as mutually agreed in a SOW.”
General Provisions - IT: 16. Inspection, Acceptance and Rejection	Inspection, Acceptance and Rejection does not apply to PaaS. Once the customer purchases PaaS, the service begins and includes a mutually agreed to stabilization period depending upon the complexity of application environment to resolve open issues. 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 PaaS. Records relating to multi-tenant usage will not be made available, due to confidentiality concerns.



# Internet Association

April 8, 2016

Department of General Services  
Procurement Division  
707 Third Street, Second Floor  
West Sacramento, CA 95605

**RE: The Internet Association's Comments on DGS's Draft Special Provisions for Cloud Computing Services for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and revisions to Special Provisions for Software as a Service (SaaS)**

To Whom it May Concern:

The Internet Association is pleased to provide the comments below regarding the Department of General Services' draft Special Provisions for Cloud Computing Services for IaaS and PaaS and draft revisions to Special Provisions for SaaS. We look forward to further discussions with the Department as it continues working to develop procurement strategies and acquisition approaches to purchase software, infrastructure, and platform cloud computing services.

The Internet Association unites the interests of leading global Internet companies and their global community of users. The Internet Association is dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users.

## **General Comments**

Buying cloud services is unlike most traditional technology purchases in government because of its rapid scalability, on-demand delivery, and pay-as-you-go pricing model. As California shifts towards this new way of obtaining computing software, infrastructure, and platforms, the State needs to design their cloud procurement strategies and solicitations so they are able to harness the full power of this model. As cloud is increasingly adopted in California and elsewhere throughout the country, traditional commodity-based acquisition strategies have the potential to be barriers to an optimized procurement of cloud services. Updated procurement strategies can foster faster, more flexible acquisition processes, which can result in an optimized use of the cloud.

As a blueprint to achieve these results, we would urge DGS to closely follow the recommendations outlined in the Center for Digital Government's [report](#) on model terms for

cloud procurement. This report was a product of collaboration between numerous state and local governments and industry representatives and highlights the need for flexible and nimble procurements.

Flexible procurements of cloud services are driving benefits around the country. A few examples are in order that highlight how different government entities are embracing and benefitting from commercial cloud services:

#### *The United States Navy's "Cloud Store"*

- The Navy has declared that it intends to move 75 percent of its data into commercial hosting environments by 2022. The "Cloud Store" allows Navy commands to easily choose from among several commercial cloud service providers once they have drawn up a solid business case for moving a given application out of government data centers. This transition process will also be allowed to occur without having to go through the cumbersome procurement and security approvals each time.

#### *The Canadian Government Embraces the Cloud*

- The Canadian government's Managed Web Services contract, which was awarded to a U.S. cloud services company last fall, aims to consolidate some 1,500 Canadian government websites into a single portal.

#### *California's New Child Welfare System*

- After years of failed attempts with traditional procurements, the State has revamped its procurement process for the new Child Welfare System, implementing a modular, agile approach to delivering government technology.

As California continues its efforts to move more fully to cloud services by developing these Special Provisions, we urge you to consider the following issues:

1. *Avoid Limiting Choices By Being Too Proscriptive*— Successful cloud procurement strategies focus on overall performance-based requirements. Recognizing that cloud is procured as a commercial item, acquisitions should leverage the Cloud Service Provider's (CSP) established commercial best practices for data center operations. A predetermined set of requirements meant to apply across all providers for all services and use cases will not result in an expeditious, cost-efficient process. CSP offerings are inherently commercial. Their shared architecture and infrastructure nature delivers tremendous benefits to users, however it requires the provider to deliver the services in a uniform manner to all customers – a manner that will vary from provider to provider and from service to service. This variation is not something the State should be concerned with – the State should rather focus on ensuring that the commitments given and precautions taken by a service provider for a given service are appropriate to the nature of the service. By stating requirements in commercial cloud industry-standard terminology and permitting the use of commercial practices, the State will have access to the most innovative and cost effective solution options.

2. *Commercial item terms* – The State’s contracting documents should recognize that most cloud services are procured as a commercial item. Broadly speaking, cloud services are sold, leased, licensed or otherwise offered for sale to the general public. This status is most easily demonstrated by a commercial sales history and publically available pricing. A commercial item approach allows all parties to extract the full scale and flexibility of the cloud. Because CSP’s are providing their services at the same high scale to potentially hundreds of thousands of customers, the services cannot be modified for specific discrete terms of a single contract.

The U.S. federal government has a published acquisition policy which favors the purchase of commercial items as opposed to items developed exclusively for government. This policy is designed to take full advantage of available and evolving technological innovations in the commercial sector and allows for commercial terms to be accepted by the government without extraneous provisions and contractual constraints related to how the services function or are provided. The federal government’s approach acknowledges that CSP terms and conditions are integral to the service, innovation and value they provide. Therefore, the federal government focuses its contractual requirements, to the maximum extent practicable, on those contract clauses needed to implement law, regulation, or executive order or determined to be consistent with customary commercial practice.

For additional information on U.S. government commercial acquisition policy, please refer to Federal Acquisition Regulation (FAR) Subpart 12.3—Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Items and the Federal Acquisition Streamlining Act (FASA) at the following link:

<http://www.acquisition.gov/far/html/FARTOCP12.html>.

3. *Evolving service terms and conditions* – A major value of the cloud is that services are continually evolving and adding enhanced features and efficiencies. Therefore, contracts for cloud services should not mandate specific technologies or methodologies. Static service terms that are more typical in traditional procurements will oftentimes be too restrictive for cloud services, unnecessarily causing potentially valuable service providers to self-select themselves out of offering their services to the State. This is because when an update or new functionality is implemented, the CSP cannot be prohibited by a contract with a given customer from upgrading its services across its customer-base. California benefits when its CSPs are able to rollout new functionality, features and security, but rigid contracts hinder the CSP’s ability to do so.
4. *Security, privacy and audit*—The key to contracting for and analyzing security, privacy and audit rights in the cloud, is recognizing the extensive amount of information already available. By leveraging established and respected standards the State can save money and be satisfied that its CSPs are secure. For example, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, DIACAP, are all standards that the State can use to quickly and reliably evaluate a CSPs security level, provided the State is thoughtful and flexible in determining what types of protections and certifications are appropriate to a particular service.

The State should be cautious about defaulting to the highest possible security requirements without an analysis of the particular service, service provider and use case. CSPs sell to a wide array of customers in different industries, for a variety of service types that is growing at an incredibly rapid pace. Trying to establish a uniform standard for every conceivable cloud service will unnecessarily increase cost and limit solution options.

We again would like to thank you for the opportunity to provide these comments and look forward to further opportunities to discuss our issues with the Special Provisions with the Department. If you have any questions, please do not hesitate to reach me at (916) 498-3316 or [callahan@internetassociation.org](mailto:callahan@internetassociation.org).

Sincerely,

A handwritten signature in black ink, appearing to read "Robert Callahan". The signature is fluid and cursive, with a long horizontal stroke at the end.

Robert Callahan  
Executive Director, State of California

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR PLATFORM AS A SERVICE (PaaS), 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:

“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.

- a. “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.
- b. “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.
- c. “Non-Public Data” means data submitted to the Service Provider’s PaaS service, 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.
- d. “Personal Data” means data submitted to the Service Provider’s PaaS service 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.
- e. “Platform-as-a-Service” (PaaS) means 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.
- f. “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.
- g. “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, that is stored on~~ the Service Provider’s hardware or exists in any system owned, maintained or otherwise controlled by the ~~State or by the~~ Service Provider, used to provide the PaaS service to the State.[GH1]
- h. “State Identified Contact” means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.
- i. “Security Incident” means the ~~reasonably suspected potentially~~ unauthorized access to, ~~Personal Data or Non-Public Data the Service Provider believes could reasonably result in the use or,~~ 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.
- j. “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.
- k. “Service Provider” means the Contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Contract.

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

- i. ~~“Statement of Work” (SOW) means a written statement in a solicitation document or Contract that describes the Service to be provided by the Contractor to the State’s service needs and expectations.~~[GH2]

## 2. DATA OWNERSHIP:

The State will own all right, title and interest in State Data that is ~~submitted 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 ~~and to provide the PaaS services~~, (2) ~~to prevent and~~ 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 ~~designed~~ 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 ~~as applicable to the Service Provider and subject to the State’s compliance in its use of the PaaS services~~:

- 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 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, ~~as documented in the SOW and/or SLA~~. The SOW and/or SLA will specify ~~whether the PaaS services include encryption as a feature and~~ 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.[tm3]
- d. Encryption of Data at Rest: ~~If the SOW and/or SLA provide for encryption of data at rest as the responsibility of the Service Provider,~~ ~~the Service Provider~~ ~~where applicable~~ shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data and Non-Public Data, unless the Service Provider presents a justifiable position approved by the State that Personal Data and Non-Public Data must be stored on a Service Provider portable device in order to accomplish work as defined in the SOW and/or SLA.
- e. 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 ~~in the SOW and/or SLA~~ and made a part of this Contract.
- f. ~~At no time shall any Personal Data and Non-Public Data or processes — which either belong to or are intended for the sole 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 with a third party without the express written consent of the State except as permitted in Section 2 above.~~[tm4]

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

- a. Incident Response: The Service Provider may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing Security Incidents with the State should be handled on an urgent as-needed basis, as part of Service Provider communication and mitigation processes as mutually agreed, defined by law or contained in the Contract.

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

- b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor/Service Provider shall promptly, but in no event in more than 48 hours, after becoming aware of a Security Incident ~~immediately~~ [GH5] report such a Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA.
- c. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed Data Breach that affects the security of any State content that is subject to applicable Data Breach notification law, the Service Provider shall (1) promptly notify the appropriate State Identified Contact within 4824 hours or sooner, 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 promptly, but in no event in more than 48 hours, after becoming aware, immediately [GH6] 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 Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall promptly notify the appropriate State Identified Contact within 4824 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, including 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 to the State. It will do so in the same manner it provides updates to similarly impacted customers and, in connection with the purchase of support options as detailed in the SOW, the Service Provider will provide updates more frequently, 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. [j7]
- d. Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair PaaS 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, if any, or to have measures in place to otherwise prevent its release, the Service Provider shall bear the costs associated with (1) its ~~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:

To the extent legally permitted, ~~T~~he 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 will/might reasonably require access to the 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. To the extent legally permitted, Service Provider agrees to use commercially reasonable efforts 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. [j8] Service Provider shall not respond to legal requests directed at the State (as opposed to Service Provider) 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 and prior to the effective date of termination, Service Provider shall make available to assist the State for in-extracting and/or transitioning, all State Data in the commonly used format by the Service Provider ~~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.

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

- c. During the Transition Period, PaaS and State Data access shall continue to be made available to the State without alteration, except as otherwise expressly permitted herein.
- d. Service Provider agrees to compensate the State for damages or losses the State incurs as a result of Service Provider's material 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 Service Provider shall not take any action to intentionally erase any State Data.
- g. The Service Provider will impose no fees for normal access and retrieval of digital content to the State.
- 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.~~ State Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods in accordance with the SOW. Certificates of destruction shall be provided to the State upon the State's written request.

## 9. **BACKGROUND CHECKS:**

As permitted by law, the Service Provider shall conduct criminal background checks and not ~~knowingly permit utilize~~ any staff, including subcontractors, to ~~have logical access to Personal Data and Non-Public Data 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~~. 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 in a format as specified in the SOW and/or SLA and agreed to by both the Service Provider and the State. Reports will include statistics and access logs as set forth in the SLA or SOW [latency statistics, user access, user access IP address, user access history and security logs for all State files related to this Contract.] [j9]~~
- 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:**

Upon request the Service Provider will make available to the State copies or summaries of its regularly performed certifications or audit reports which it makes available to customers (e.g., ISO 27001, Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit reports), which will serve as the primary method for the State to verify conformance with the Service Provider's obligations. Additionally, if necessary to supplement such certifications or audit reports the Service Provider shall allow the State to audit conformance to the Contract terms subject to reasonable time, place, scope, manner and frequency. The State may perform this audit or Contract with a third party at its discretion under terms of confidentiality 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 as set forth in the SOW. The Service Provider shall provide a redacted version or a summary 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. [GH10]

## 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 planned downtime for upgrades (e.g., major upgrades, minor upgrades, system changes) that is expected to materially and negatively 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.[tm11]

## 14. **SECURITY PROCESSES:**

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

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 to the extent mutually agreed by the parties, and limit staff knowledge of State Data to that reasonably required ~~which is absolutely necessary~~ to perform job duties. [tm12]

## 16. IMPORT AND EXPORT OF DATA:

The State shall have the ability to import or export data State Data in the PaaS service in whole or in part at its discretion without interference from the Service Provider in accordance with the SOW. ~~This includes the ability for the State to import or export data to or from other Service Providers.~~ [GH13]

## 17. RESPONSIBILITIES AND UPTIME GUARANTEE:

The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support necessary to provide the PaaS related to the services in accordance with this Contract and the SOW being provided. The technical and professional activities required for establishing, managing and maintaining the environment necessary to provide the PaaS services in accordance with this Contract and the SOW are the responsibility of the Service Provider. Service Provider shall use commercially reasonable efforts to make the PaaS services available 24/7/365 (with agreed-upon maintenance downtime), and shall provide service to customers as defined in the SOW and/or SLA. [j14]

## 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.~~ [GH15]

## 19. RIGHT TO REMOVE INDIVIDUALS: [GH16]

The State shall have the right at any time to request the Service Provider remove from interaction with State any Service Provider representative who the State reasonably 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 promptly ~~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. This Section 19 shall apply only to individuals who (i) visit the State's offices or facilities in the course of providing the PaaS services or (ii) are dedicated exclusively to providing the PaaS services to the State. The State acknowledges that although Service Provider will respond promptly to such requests, agreeing to remove such individuals may result in delays in the performance of Service Providers obligations hereunder and Service Provider will have no liability for any such delays.

## 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 which reflects 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 use commercially reasonable efforts to notify the State using 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 forty-eight twenty-four (48/24) 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 to the extent available at the time of the notification:
  - 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 in accordance with its Business Continuity and Disaster Recovery Plans restore continuity of PaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair PaaS as

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

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. Service Provider shall conduct an investigation of the disaster or catastrophic failure and shall share a summary of the report of the investigation with the State upon written request. The State and/or its authorized agents shall have the right to lead (if required by law) or reasonably participate, in Service Provider's discretion, in the investigation. Service Provider shall reasonably cooperate ~~fully~~ with the State, its agents and law enforcement.

## 21. COMPLIANCE WITH ACCESSIBILITY STANDARDS:

The Service Provider shall provide the State upon written request with its Voluntary Accessibility Templates that set forth the extent to which it satisfies the internationally recognized best practices in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA~~comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.~~

## 22. WEB SERVICES:

The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible.[GH17]

DRAFT

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR PLATFORM AS A SERVICE (PaaS), 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. "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.
- e. "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.
- f. "Platform-as-a-Service" (PaaS) means 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.
- 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.

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

- 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.
- 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 PaaS 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. Encryption of Data at Rest: The Service Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data and Non-Public Data, unless the Service Provider presents a justifiable position approved by the State that Personal Data and Non-Public Data must be stored on a Service Provider portable device in order to accomplish work as defined in the SOW and/or SLA.
- e. 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.

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

- f. 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:

Unless otherwise specified in the SOW, 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<sup>[NS2]</sup>. 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, Service Provider and contractors to access State Data remotely only as required to provide technical or customer<sup>[NS3]</sup> 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 or provided in an SOW<sup>[NS4]</sup>.

#### 5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

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

- a. Incident Response: The Service Provider may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing Security Incidents with the State should be handled on an urgent as-needed basis, as part of Service Provider communication and mitigation processes as mutually agreed, defined by law or contained in the Contract.
- b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall ensure the Service Provider shall immediately reports a Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA.
- c. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed Data Breach that affects the security of any State content that is subject to applicable Data Breach notification law, the Contractor shall ensure the Service Provider shall (1) promptly notify-notifies the appropriate State Identified Contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) takes 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 notify-notifies 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 notify-notifies 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) cooperates with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implements necessary remedial measures, if necessary; and (3) documents 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 provides 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.

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

- d. The Contractor shall ensure Service Provider ~~shall~~ quarantines the Data Breach, ensures secure access to Data, and repairs PaaS 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 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 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<sup>[NS5]</sup> 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, PaaS 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~~<sup>[NS6]</sup> 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<sup>[NS7]</sup> permitted by law, the Contractor shall ensure the Service Provider ~~shall~~ conducts 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

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

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 in a format as specified in the SOW and/or SLA and agreed to by both the Service Provider and the State. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this Contract.
- 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 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. <sup>[NS8]</sup> 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 <sup>[NS9]</sup> Service Provider ~~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 ~~Service Provider~~ Contractor 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 <sup>[NS10]</sup> 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.

## 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 <sup>[NS11]</sup> 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:

# STATE MODEL

## CLOUD COMPUTING SERVICES SPECIAL PROVISIONS

### (Platform as a Service)

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:

The State shall have the right at any time to ~~require request~~ 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 ~~Service Provider~~Contractor 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~~ [NS12]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: [NS13]

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 notify notifies~~ the State by ~~the fastest means available~~[NS14] 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~~ Service Provider ~~shall restores~~ continuity of PaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair PaaS 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.

#### 21. COMPLIANCE WITH ACCESSIBILITY STANDARDS:

The ~~Contractor shall ensure the~~ Service Provider ~~shall comply complies~~ with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of

# STATE MODEL CLOUD COMPUTING SERVICES SPECIAL PROVISIONS (Platform as a Service)

---

1973.

## 22. WEB SERVICES:

The Contractor shall ensure the Service Provider ~~shall~~ uses Web services exclusively to interface with State Data in near real time when possible.

DRAFT