

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

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR SOFTWARE AS A SERVICE (SaaS), 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) "Cloud Software as a Service (SaaS)" - The capability provided to the consumer is to use applications made available by the provider running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- b) "Cloud Platform as a Service (PaaS)" - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- c) "Cloud Infrastructure as a Service (IaaS)" - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
- d) "Data" - means any State information, formulae, algorithms, or other content that the State, the State's employees, agents and end users access, upload, create or modify using the SaaS pursuant to this Contract. Data also includes user identification information which may contain Data or from which the State's Data may be ascertainable. The State or its end users is the controller and which Contractor processes Data in the course of providing SaaS. The terms "controller", "processor", "process", "processed", "processing", and "personal data" used in this Contract shall be as defined by EU Directive 95/46/EC, unless otherwise defined by applicable data protection legislation.

Comment [A1]: Restrict to State related data, and exclude public information.

- e) "Data Breach" - means ~~any the confirmed unauthorized access, that results in the~~ destruction, loss, theft, use, modification or disclosure of Data ~~by an unauthorized party or that is in violation of Contract terms and/or applicable state or federal law.~~

Comment [A2]: Sentence restructured to restrict to confirmed unauthorized access and results.

- f) ~~"Security Incident" means the potentially unauthorized access to Data the Contractor believes could reasonably result in the use, disclosure or theft of the State's unencrypted Data within the possession or control of the Contractor. A Security Incident may or may not turn into a Data Breach.~~

2. SaaS AND DATA AVAILABILITY:

Unless otherwise stated in the Statement of Work,

- a) The Data shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).
- b) If Data monthly availability is less than 100% (excluding agreed-upon maintenance downtime), the State shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the Statement of Work if the State is unable to access the Data as a result of:
 - 1) Acts or omission of Contractor;
 - 2) Acts or omissions of third parties working on behalf of Contractor;
 - 3) Network compromise, network intrusion, hacks, introduction of viruses, disabling devices, malware and other forms of attack that can disrupt access to Contractor's server, to the extent such attack would have been prevented by Contractor taking reasonable industry standard precautions;
 - 4) Power outages or other telecommunications or ~~Internet-network~~ failures, to the extent such outages were within Contractor's direct or express control.

- e) ~~If Data monthly availability is less than 100% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may terminate the contract for material breach in accordance with the Termination for Default provision in the General Provisions - Information Technology.~~

Comment [A3]: Each SaaS offering will include appropriate SLA, with its applicable availability milestones. Not all offerings are "mission critical", therefore the standard should be appropriate for the offering. The State always has the ability to terminate if unhappy with the service.

- f) ~~Contractor shall provide advance written notice to the State in the manner set forth in the Statement of Work of any major upgrades or changes that will affect the SaaS availability.~~

1. SaaS AND DATA SECURITY:

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

a) In addition to the Compliance with Statutes and Regulations provision set forth in the General Provisions – Information Technology, Contractor shall ~~certify to the State:~~

~~1) Implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Data. Such security measures shall be identified in the Statement of Work for the particular service and consistent with the Contractor's representations concerning the technology environment being provided. The Contractor 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 Contractor unless the parties have expressly agreed to do so in writing. The sufficiency of its security standards, tools, technologies and procedures in providing SaaS under this Contract;~~

~~2) Compliance with the following:~~

- ~~i. The California Information Practices Act (Civil Code Sections 1798 et seq.);~~
- ~~ii. NIST Special Publication 800-53, Revision 4 or its successor;~~
- ~~iii. Undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit. Audit results and Contractor's plan to correct any negative findings shall be made available to the State upon request; and~~
- ~~iv. Privacy provisions of the Federal Privacy Act of 1974;~~
- ~~v. All other applicable industry standards and guidelines, including but not limited to relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines.~~

b) Contractor shall implement and maintain all appropriate administrative, physical, technical and procedural safeguards in accordance with section a) above at all times during the term of this Contract to secure such Data from Data Breach, protect the Data and the SaaS from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data ~~to the extent it is under the control of the Contractor.~~

c) Contractor shall allow the State reasonable access to SaaS security information, latency data, and other related SaaS security data that affect this Contract and the State's Data, at no cost to the State ~~to the extent available under the service.~~

d) ~~Contractor assumes responsibility for the security and confidentiality of the Data under its control. The State will be the Data Controller of its data at all times and appoints Contractor as a processor of Data in connection with the services. The Contractor will not access State user accounts or State Data, except (1) in the course of data center operations, (2) 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. The State has sole responsibility for the accuracy, quality, and legality of any State provided Data, including the means by which it was obtained by the State.~~

e) No Data shall be copied, modified, destroyed or deleted by Contractor other than for normal operation or maintenance of SaaS during the Contract period without prior written notice to and written approval by the State identified contact.

f) Remote access to Data from outside the continental United States, including remote access to Data by authorized SaaS support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Security Officer.

2. ENCRYPTION:

a) Unless otherwise stipulated, 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.

b) ~~Encryption of Data at Rest: Where provided as part of the services, the Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Data, unless the Contractor presents a justifiable position approved by the State that Data must be stored on a Contractor portable device in order to accomplish work as defined in the SOW and/or SLA.~~

3. DATA LOCATION:

Unless otherwise stated in the Statement of Work and approved in advance by the State Chief Information Security Officer, the physical location of Contractor's data center where the Data is stored shall be within the continental United States.

4. RIGHTS TO DATA:

The parties agree that as between them, all rights, including all intellectual property rights, in and to Data shall remain the exclusive property of the State, and Contractor has a limited, non-exclusive license to access and use the Data as provided to Contractor solely for performing its obligations under the Contract. Nothing herein shall be construed to confer any license or right to the Data, including user tracking and exception Data within the system, by implication, estoppel or otherwise, under copyright or other intellectual property rights, to any third party. Unauthorized use of Data by Contractor or third parties is prohibited. For the purposes of this requirement, the phrase "unauthorized use" means the data mining or

Comment [A4]: It is unclear what the list of a few odds and ends of standards accomplishes. The vendor should comply with statute, all statutes, so listing those is not necessary. NIST 800-53 is not a set of technical standards, but a process to review standards to determine which ones are applicable and necessary. SaaS vendor should have a SSAE 16 audit completed and provide the State with evidence of completion. This should just be a requirement, not something that the vendor complies with.

Comment [A5]: Not all SaaS engagements would collect and be able to provide this information.

Comment [A6]: Clarifies that the State is and remains the Data Controller. This will benefit both parties if State Data is subpoenaed from the Contractor.

Comment [A7]: Not all services will require or have hard drive encryption available as an option. The State may decide not to use hard drive encryption for any number of reasons.

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

processing of data, stored or transmitted by the service, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security or service delivery analysis that is not explicitly authorized.

5. TRANSITION PERIOD:

- a) ~~To the extent available as part of the services, f~~For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Contractor shall assist the State in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
- b) The Transition Period may be modified in the SOW or as agreed upon in writing by the parties in a contract amendment.
- c) During the Transition Period, SaaS and 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.
- d) ~~Contractor agrees to compensate the State for damages or losses the State incurs as a result of Contractor'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) _____ Upon written confirmation by the State, that it has taken possession of the data, the Contractor shall permanently destroy or render inaccessible any portion of the Data in Contractor's and/or subcontractor's possession or control in accordance with NIST approved methods. Within thirty (30) days, Contractor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
- f)e) _____ The State at its option, may purchase additional transition services as agreed upon in the SOW.
- g)f) _____ After termination of the Contract and the prescribed retention period, the Contractor shall securely dispose of all State Data in all forms. 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.

Comment [A8]: The State always retains its contractual rights to recovery for the failure of Contractor to perform its obligations. It does not need to be stated in the contract to protect that right.

6. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

- The Contractor shall inform the State of any ~~Security Incident or Data~~ Breach related to State Data within the possession or control of the Contractor and related to the service provided under this Contract.
- a) ~~Incident Response: The Contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing Security Incidents with the 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 set forth in the SOW and/or SLA, the Contractor shall promptly 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.~~
 - c)a) _____ Breach Reporting Requirements: If the Contractor has actual knowledge of a ~~confirmed~~ Data Breach that affects the security of any State Data that is subject to applicable Data Breach notification law, the Contractor shall (1) promptly notify the appropriate State Identified Contact ~~within 24 hours or sooner, unless otherwise required by applicable law,~~ and (2) take commercially reasonable measures to address the Data Breach in a timely manner. ~~Unless otherwise required by law, t~~The State's Chief Information Security Officer , or designee, shall determine whether notification to the individuals whose Data has been lost or breached is appropriate.

Comment [A9]: Security Incident reporting will provide the State with large amounts of unintelligible data. Service Providers are subject to network pings and attempted attacks hundreds of times each day. The State should be concerned when the vendor's defenses do not prohibit a breach, which is why breach notification is left as a contractual requirement. If there are cases where some additional security log reporting is important, it should be defined in the SOW/SLA. 8.a. and 8.b. removed, on basis of above statement.

7. 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 otherwise set forth in in the SOW and/or SLA, shall promptly notify the appropriate State Identified Contact ~~within 24 hours or sooner by telephone, unless shorter time is required by applicable law,~~ if it confirms that there ~~is or reasonably believes that there~~ has been a Data Breach. The Service Provider shall (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business ~~practices in providing the services,~~ if necessary.
 - b) ~~Service Provider will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service Provider to the State Identified Contact until the Data Breach has been effectively resolved to the State's satisfaction.~~
 - c) ~~Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair IaaS and/or 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.~~
 - d)b) _____ Unless otherwise set forth in the SOW and/or SLA, if a Data Breach is a direct result of the Service Provider's breach of its ~~Contract~~ contractual obligation to encrypt Personal Data and/or Non-Public Data ~~or otherwise prevent its release,~~ the Service Provider shall bear the costs

Comment [A10]: The Vendor may need to focus on fixing the problem more than notification in the first few hours of a confirmed breach. The State should receive prompt notice which takes into consideration any other factors which may occur, including the State being unable to receive the communication.

Comment [A11]: This should be limited to confirmed breaches, and prompt notice should be sufficient.

Comment [A12]: The State may have to change business practices.

Comment [A13]: The format and frequency of updates should be left to the parties in the situation.

Comment [A14]: The Service Provider's obligation is to provide what is required under the contract. If it doesn't provide what is required under the contract, then the State has all of the contractual and legal remedies available to it for that failure. This doesn't require language in the contract to preserve that right.

Comment [A15]: Grammatical revision.

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

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.

8. DISASTER RECOVERY/BUSINESS CONTINUITY:

Unless otherwise stated in the Statement of Work,

a) ~~In the event of disaster or catastrophic failure that results in significant Data loss or extended loss of access to Data, Contractor 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. Contractor shall provide such notification within twenty-four (24) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. To the extent possible, in the notification, Contractor shall inform the State of:~~

- 1) The scale and quantity of the Data loss;
- 2) What Contractor has done or will do to recover the Data and mitigate any deleterious effect of the Data loss; and
- 3) What corrective action Contractor has taken or will take to prevent future Data loss.
- 4) ~~Contractor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.~~

b) Contractor shall restore continuity of SaaS, restore Data in accordance with the SOW and/or SLA, restore accessibility of Data, and repair SaaS as needed to meet the performance requirements stated in the SLA. ~~Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.~~

c) Contractor 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. Contractor shall cooperate fully with the State, its agents and law enforcement.

9. EXAMINATION AND AUDIT:

a) The Contractor shall provide reports to the State in a format as specified in the SOW and/or SLA and agreed to by both the Contractor 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.

10. CONTRACT AUDIT:

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

11. DISCOVERY:

Contractor shall promptly notify the State upon receipt of any requests which in any way might reasonably require access to the Data of the State or the State's use of the SaaS. Contractor 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, unless prohibited by law from providing such notification. Contractor shall provide such notification within forty-eight (48) hours after Contractor receives the request. Contractor shall not respond to subpoenas, service of process, Public Records Act requests, and other legal requests directed at Contractor regarding this Contract without first notifying the State unless prohibited by law from providing such notification. Contractor 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. Contractor shall not respond to legal requests directed at the State unless authorized in writing to do so by the State.

14. LIMITED USE:

~~Products and services provided under these terms are for the State's internal use and not for further commercialization. Unless otherwise stated in the Statement of Work, the State will not: (i) sell, resell, license, sublicense, lease, rent or distribute SaaS or include SaaS as a service bureau or outsourcing offering, or make any position of SaaS available for the benefit of any third party; (ii) copy or reproduce any portion, feature, function, or user interface of SaaS; (iii) interfere with or disrupt the integrity or performance of the SaaS; (iv) use SaaS to submit, send or store Data that is infringing, obscene, threatening, libelous or otherwise unlawful or tortuous material or material in violation of any third party's privacy rights; (v) access SaaS to build a competitive product or service, or (vi) reverse engineer SaaS. State is responsible for complying with all terms of use for any software, content, service or website it loads, creates or accesses when using SaaS. The State is responsible for complying with applicable laws and regulations, including but not limited~~

Comment [A16]: Sentence structure update. In addition, you have already set up the contractual duties for State Data and security to be identified in the SOW, so a breach of those contractual duties is what should be covered by this paragraph.

Comment [A17]: The Vendor may need to focus on fixing the problem more than notification in the first few hours of a confirmed breach. The State should receive prompt notice which takes into consideration any other factors which may occur, including the State being unable to receive the communication.

Comment [A18]: The State always has the right to pursue its contractual remedies if the Contractor fails to meet the requirements of the contract.

Comment [A19]: The State always has the right to pursue its contractual remedies if the Contractor fails to meet the requirements of the contract.

Comment [A20]: Service Providers have to limit use of the services to the State and ensure compliance with applicable laws.

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

to, obtaining any required export or import authorizations if the State exports, imports or otherwise transfers products or deliverables provided under Contract.

15. SUSPENSION OF SERVICES:

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.

16. SaaS OPERATIONS:

Unless otherwise stated in the Statement of Work, Contractor retains sole control over the operation, provision, maintenance and management, and performance of SaaS, including the selection, deployment, modification and replacement of the Software and/or SaaS materials, and maintenance, upgrades, corrections or repairs; and (ii) reserves the right to make any changes to SaaS that it deems necessary or useful to maintain or enhance the quality or delivery of Contractor's services to its customers, the competitive strength of or market for Contractor's services, or SaaS' cost efficiency or performance.

17. GLOBAL TRADE COMPLIANCE:

Imports, exports and other transfers of data or software stored, used or processed using the services 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 in the U.S. Treasury Department's List of Specialty 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.

18. EUROPEAN PERSONAL DATA:

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 Contractor, and provide whatever information Contractor reasonably requests related to that storage or processing. Upon the State's request, Contractor will enter into (or cause its Affiliates to enter into) EU Model Contract(s) with appendices (including technical and organization security measures) in the form from time to time used by the Contractor and its Affiliates (and available to the State upon request). The State appoints Contractor as its agent to execute EU Model Contracts on the State's behalf.

Comment [A21]: This provision covers the grounds for suspension of services.

Comment [A22]: This ensures the Service Provider's compliance with global trade restrictions.

Comment [A23]: While it may not be common, if the State Data contains personal information on European citizens, there may be additional legal requirements.

Comments to State Model Cloud Computing Services Special Provisions (Software as a Service)

Workday respectfully requests that the State consider the following prior to finalizing its SaaS provisions.

Section 3:

- Is it the State’s intention that by certifying the sufficiency of security standards, tools, technologies and procedures the Contractor is to indemnify the State against all data breaches, whether caused by the Contractor’s failure to use its stated methods or through other means? We are not aware of any vendor who would guarantee that there will never be a security breach or take responsibility for all security breaches, however caused. That is the role of an insurer. **We suggest rewording to remove the ambiguity of what “certify” means in this context.**
- Section (2)(ii) requires NIST compliance even though there are other data security standards appropriate for Cloud computing. This would eliminate many vendors from consideration, including vendors who are headquartered in California and employ thousands of Californians. **We suggest rewording to allow NIST as one of several acceptable standards.**
- Section (b) also contains language which suggests that the Contractor has an absolute obligation to secure data and accordingly is responsible for any data security breach, no matter how caused. We are not aware of any vendor who would guarantee that there will never be a security breach or take responsibility for all security breaches, however caused. That is the role of an insurer. **We suggest rewording to change the obligation, which may be redundant to what is already in (a).**
- Section (d) also states that the contractor has responsibility for the security and confidentiality of Data. Again, we are not aware of any vendor who would guarantee that there will never be a security breach or take responsibility for all security breaches, however caused. That is the role of an insurer. **We suggest rewording to change the obligation, which may be redundant to what is already in (a).**
- (c) calls for broad access to security data. This is not a best practice for security since broad dissemination of information about security protocols is a good way to have them fall into the wrong hands. **We suggest rewording to provide access to security audit reports and to security information related to a Data Breach that impacted the State’s Data and is necessary for remediation or mitigation.**
- Accordingly, we suggest the following changes to 3:

3. **SaaS AND DATA SECURITY:**

a) In addition to the Compliance with Statutes and Regulations provision set forth in the General Provisions – Information Technology, ~~Contractor shall certify to the State~~ the SOW shall include:

- 1) ~~The sufficiency of its security standards, tools, technologies and procedures in providing SaaS under this Contract;~~ A commitment to adhering to a security policy and procedures reasonably expected to secure the State's Data in Contractor's control or possession.
- 2) Such policy and procedures shall include the following, as may be applicable depending upon the types of State Data being stored ~~Compliance with the following:~~
 - i. The California Information Practices Act (Civil Code Sections 1798 et seq.);
 - ii. A recognized data security standard for Cloud such as NIST Special Publication 800-53 Revision 4 or its successor, the ISO 27001 and 27018 standards or their successors, or another equivalent standard approved by the State;
 - iii. Undergoing an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit. Audit results and Contractor's plan to correct any negative findings shall be made available to the State upon request; and
 - iv. Privacy provisions of the Federal Privacy Act of 1974;
 - v. All other applicable industry standards and guidelines, including but not limited to relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines.

b) Contractor shall implement and maintain ~~all~~ appropriate administrative, physical, technical and procedural safeguards in accordance with section a) above at all times during the term of this Contract, reasonably designed to secure such Data from Data Breach, protect the Data and the SaaS from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data.

c) Contractor shall allow the State reasonable access to SaaS security audit reports ~~information~~, latency data related to SLA commitments, and ~~other related~~ SaaS security data related to mitigation and resolution of any Data Breach involving ~~that affect this Contract and~~ the State's Data, at no cost to the State.

~~d) Contractor assumes responsibility for the security and confidentiality of the Data under its control.~~

~~e) d)~~ No Data shall be copied, modified, destroyed or deleted by Contractor other than for normal operation or maintenance of SaaS during the Contract period without prior written notice to and written approval by the State identified contact.

~~f) e)~~ Remote access to Data from outside the continental United States, including remote access to Data by authorized SaaS support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Security Officer.

•

Section 7:

- Section (e) requires the NIST standard when other secure means are available. We suggest replacement of “NIST approved methods” with “NIST approved methods or other industry-accepted standards for secure deletion of confidential and sensitive data.”
- Section (e) also requires an absolute destruction from all media, including backup media, within the 30 day period. This will drive up expenses for the State because most vendors do not destroy data on backup media outside of their normal backup destruction cycles. Please add the following, “Contractor will not be required to destroy Data from its backup media and servers until such time as the backup copies are scheduled to be deleted or destroyed, and shall continue to protect the Data in accordance with this Agreement until such deletion or destruction.”
- Section (g) appears to be either in conflict with or redundant to section (e). We suggest deletion of (g).

Section 8:

- “Security Incident” is broadly defined as “potentially unauthorized access. . .” This is used in Section 8 to require prompt reporting of potential, rather than actual, unauthorized access. The problem with reporting “potential” issues is twofold. First, it creates its own risks because disclosure of an identified vulnerability that has not been exploited is itself a security risk; there is no assurance that the systems of customers who receive this information are themselves appropriately secured. Second, it would create a series of false alarms which can dilute the importance of a real data breach notice. As a very real example, phishing incidents are often focused on obtaining single sign-on login credentials from users. If a user discovers that their own account has been compromised, it may take some time to determine that the compromise comes from unauthorized use of login credentials obtained during a phishing incident rather than an actual breach of a vendor’s security. **We suggest that “Security Incident” be used in a different manner; a Security Incident that is not resolved within a stated amount of time must be treated as a reported Data Breach.**
- A genuine data breach for a Cloud SaaS provider is likely to impact a large number of customers. In such a situation, it is important for the Cloud SaaS provider to have consistent obligations to all customers. **We suggest that all of Section 8 be phrased as “Unless otherwise stated in the Statement of Work.”**
- The 24 hour breach reporting requirement is shorter than required under any existing state law; we believe that the earlier of 48 hours or as required by applicable law will allow vendors to avoid false alarms by providing adequate time to investigate.
- Accordingly, we suggest the following changes to Section 8:

8. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

Unless otherwise stated in the Statement of Work, the following shall apply: The Contractor shall inform the State of ~~any Security Incident or~~ Data Breach related to State Data within the possession or control of the Contractor and related to the service provided under this Contract in accordance with the following protocols.

a) Security Incident Handling: The Contractor shall promptly investigate any Security Incident to determine whether it is a Data Breach. Security Incidents which are not Data Breaches but represent an identified vulnerability within the Contractor's SaaS shall be remedied promptly with a log kept of the Security Incident and response. Security Incidents which are determined to not be either vulnerabilities or actual Data Breaches shall be noted in the Contractor's log of Security Incidents. If a Security Incident cannot be determined to be a false alarm within 48 hours of reporting, it will be deemed a Data Breach until such time as it is determined to be a false alarm and will be reported to the State as a Data Breach.

a)b) Incident Response: The Contractor may need to communicate with outside parties regarding a Security Incident or Data Breach, 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 or Data Breaches 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 set forth in the SOW and/or SLA, the Contractor shall promptly 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.~~

c) Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed Data Breach that affects the security of any State Data that is subject to applicable Data Breach notification law, the Contractor shall (1) promptly notify the appropriate State Identified Contact within ~~24~~48 hours or sooner, unless otherwise required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner. The State's Chief Information Security Officer, or designee, shall determine whether notification to the individuals whose Data has been lost or breached is appropriate.

Section 9:

- This section has inconsistent language as to whether there can be different protocols in the SLA or SOW. (a) - (d) should all be clearly indicated to be variable in the SLA or SOW. For nearly all SaaS providers, uniform obligations in the event of a security breach are essential to handling a crisis situation.

- We note that there appears to be no obligation on the part of the State to notify the Contractor of a suspected breach. It makes sense for one to be added. Our experience has been that poor safeguarding of individual login credentials is the most common cause of a limited security breach of a properly secured Cloud SaaS. (In that case, the data breach is not a vendor-caused breach but the contractor should still need to provide cooperation in mitigation/remediation efforts.)

Section 11:

- In many cases, reports of the types listed in (a) can be generated by the State and the Contractor may not have access to the Data for security purposes. Accordingly, we suggest changing (a) to add, “Such information may be made available by Contractor via reports that are generated by SaaS users, rather than by the Contractor.”

Section 12:

- True multi-tenant SaaS vendors are unlikely to agree that customers have broad system audit rights. Since contractors must already provide financial audits under the General Terms to confirm charges, and they must provide their SOC audits under Section 3, this section should be removed.