

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|----------------------------|--------------------------|--------------------------|--------------------------|--|
| <p>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:</p> <p>A. CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;</p> <p>B. CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH</p> | <p>THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR INFRASTRUCTURE AS A SERVICE (IaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). STATE AGENCIES MUST FIRST:</p> <p>A. CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;</p> <p>B. CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND</p> | <p>No Comment</p> | <p>No Comment</p> | <p>No Comment</p> | <p>No Comment</p> | <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.</p> <p>Managed service and the features that are activated depend on the options selected by the customer. (Duplicate below)</p> <p>IBM IaaS is meant to be a self-managed service and the features that are activated depend on the options selected by the customer.</p> <p>Many features described in these terms are activated only if the customer selects the feature. Some are available at an extra cost.</p> <p>These Special Provisions need to reflect the flexibility are contemplated by IaaS. Because of the unmanaged nature of IaaS, IBM cannot commit to all the terms and conditions in this document for all IaaS offered by IBM.</p> <p>For example: SOFTLAYER (self-managed) Cloud Managed Services IaaS</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|--|--|---|---|--------------------------|---|
| <p>SAM 4981.1, 4983 AND 4983.1 AND THEN;</p> <p>C. MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.</p> | <p>4983.1 AND THEN;</p> <p>C. MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.</p> | | | | | <p>has Options for High Availability, PCI, HIPAA, DR, Migration Services, zOS includes a Private Cloud Mainframe</p> <p>Additionally, similar to the SaaS Special Provision, contractors should have the ability to modify the IaaS Special Provisions in a SOW.</p> |
| <p>1. Definitions:</p> <p>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.</p> <p>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.</p> <p>c. “Individually Identifiable</p> | <p>1. Definitions:</p> <p>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.</p> <p>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.</p> <p>c. “Individually Identifiable Health Information” means Information that is a subset</p> | <p>c. Non-Public Data” means data submitted to the Service Provider’s PaaS service, other than Personal Data....</p> <p>d. Personal Data” means data submitted to the Service Provider’s PaaS service that....</p> <p>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, that is stored on the Service Provider’s hardware or exists in any system owned, maintained or otherwise controlled by the</p> | <p>a. Delete Authorized Persons - This definition is not used.</p> <p>b. “Data Breach” means the confirmed unauthorized access that results in the use, disclosure, destruction, modification, loss or theft of the State’s unencrypted Personal Data or Non-Public Data.</p> <p>Delete Individually Identifiable Health Information. - This definition is not used.</p> <p>“Protected Health Information” (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</p> | <p>1. “Service Provider” 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.</p> | <p>No Comment</p> | <p>“Authorized Users” - For PaaS/IaaS, not all the individuals identified in the definition of “Authorized Users” will have full access to PaaS/IaaS.</p> <p>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”.</p> <p>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</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|--|---|-----|-----------------------|--|
| <p>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.</p> <p>d. “Non-Public Data” means data, other than Personal Data, that is not subject to distribution to the public as</p> | <p>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.</p> <p>d. “Infrastructure-as-a-Service” (IaaS) means the capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating</p> | <p>Service Provider, used to provide the PaaS service to the State.</p> <p>i. “Security Incident” means the reasonably suspected unauthorized access to, use or disclosure....</p> <p>Statement of Work” (SOW) means a written statement in a Contract that describes the Service to be provided by the Contractor to the State’s service needs and expectations.</p> | <p>Business Associate on behalf of Covered Entity. - This is a standard definition of PHI as it applies under HIPAA</p> <p>Deleted Security Incident - Not used based on other changes.</p> | | | <p>limitation, any hypertext markup language files, scripts, programs, recordings, sound, music, graphics, images, applets, or servlets that are created, installed, uploaded, or transferred in connection with the Services by the State, users, or solution recipients</p> <p>“Security Incident” – Delete “potentially”. PaaS/IaaS 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.</p> <p>“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.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|----------------------------|-----|-----|-----------------------|-----|
| <p>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.</p> <p>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.</p> <p>f. “Platform-as-a-Service”</p> | <p>systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).</p> <p>e. “Non-Public Data” means data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, regulation or policy from access by the general public as public information.</p> <p>f. “Personal Data” means data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information</p> | | | | | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|----------------------------|-----|-----|-----------------------|-----|
| <p>(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.</p> <p>g. “Protected Health Information” (PHI) means Individually Identifiable Health Information</p> | <p>(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.</p> <p>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.</p> <p>h. “State Data” means all data created or in any way</p> | | | | | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|----------------------------|-----|-----|-----------------------|-----|
| <p>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.</p> <p>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</p> | <p>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.</p> <p>i. “State Identified Contact” means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.</p> <p>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</p> | | | | | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|--|----------------------------|-----|-----|-----------------------|-----|
| <p>Service Provider’s hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Service Provider.</p> <p>i. “State Identified Contact” means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.</p> <p>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.</p> <p>k. “Service Level Agreement”</p> | <p>control of the Service Provider. A Security Incident may or may not turn into a Data Breach.</p> <p>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.</p> <p>l. “Service Provider” means the Contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Contract.</p> | | | | | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|----------------------------|-----|-----|-----------------------|-----|
| <p>(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</p> <p>(1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure),</p> <p>(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.</p> <p>1. "Service Provider" means the Contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Contract.</p> | <p>m. "Statement of Work" (SOW) means a written statement in a solicitation document or Contract that describes the State's service needs and expectations.</p> | | | | | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|---|--|--|--|---|
| m. "Statement of Work" (SOW) means a written statement in a solicitation document or Contract that describes the State's service needs and expectations. | | | | | | |
| <p>2. Data Ownership:</p> <p>The State will own all right, title and interest in State Data that is related to the services provided by this Contract. The Service Provider shall not access State user accounts or State Data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Contract, (4) at the State's written request or (5) as required by law.</p> | <p>2. Data Ownership:</p> <p>The State will own all right, title and interest in State Data that is related to the services provided by this Contract. The Service Provider shall not access State user accounts or State Data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Contract, (4) at the State's written request or (5) as required by law.</p> | <p>The State will own all right, title and interest in State Data that is submitted 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.</p> | <p>The State will be the Data Controller of its data at all times and appoints Service Provider as a processor of Personal Data in connection with the Services.</p> <p>Clarifies that the State is and remains the Data Controller. This will benefit both parties if State Data is subpoenaed from the Service Provider.</p> | <p>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</p> | No Comment | No Comment |
| <p>3. Data Protection:</p> <p>Protection of personal privacy and data shall be an</p> | <p>3. Data Protection:</p> <p>Protection of personal privacy and data shall be an</p> | <p>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</p> | <p>The Service Provider shall implement and maintain appropriate administrative, technical and organizational security measures to</p> | <p>...of the Contractor and Service Provider to ensure there is no inappropriate or unauthorized use</p> | <p>IaaS:</p> <p>Protection of personal privacy and data shall be an integral part of the business activities of</p> | <p>PaaS</p> <p>For PaaS, safeguarding the confidentiality, integrity and availability of State information</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|---|---|--|--|--|
| <p>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:</p> <p>a. In addition to the Compliance with Statues and Regulations provisions set forth in the General Provisions – Information Technology</p> <p>i. The California Information Practices Act (Civil Code Sections 1798 et seq).</p> <p>ii. NIST Special Publication 800-53 Revision 4 or its successor.</p> <p>iii. Privacy provisions of the Federal Privacy Act of 1974.</p> <p>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</p> | <p>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:</p> <p>a. In addition to the Compliance with Statues and Regulations provisions set forth in the General Provisions – Information Technology</p> <p>i. The California Information Practices Act (Civil Code Sections 1798 et seq).</p> <p>ii. NIST Special Publication 800-53 Revision 4 or its successor.</p> <p>iii. Privacy provisions of the Federal Privacy Act of 1974.</p> <p>b. All State Data obtained by the Service Provider within its control in the performance of this Contract</p> | <p>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:</p> <p>c. Unless otherwise stipulated, Personal Data and Non-Public Data shall be encrypted 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.</p> <p>Comment: The State rightly establishes in the template that the SOW and/or SLA are the right place to set out which party is responsible for encryption. Similarly, those are</p> | <p>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.</p> <p>Deleted “a” - This is not a complete sentence and this section does not define data protection standards. These statutes and publications define areas of security concern – a checklist of items to cover - but they do not set technical standards. A Cloud provider should provide the State with the security level that it is offering and be bound to provide that level of security.</p> | <p>of State information at any time. To this end, the Contractor shall ensure the Service Provider safeguards the confidentiality, integrity and availability of State information.....</p> <p>a. All State Data obtained by the Contractor and/or Service</p> <p>f.or retained by the Contractor or Service Provider or any party related to the Contractor or Service Provider for subsequent use....</p> | <p>the Service Provider. Requirements and responsibilities for security of State Data shall be set forth in the SOW and/or SLA The Service Provider shall comply with the following conditions:</p> <p>c and d: Unless otherwise stipulated in the SOW and/or SLA,</p> <p>Unless otherwise stipulated in the SOW and/or SLA, ...</p> | <p>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</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|--|--|-----|-----------------------|--|
| <p>the State.</p> <p>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.</p> <p>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</p> | <p>shall become and remain the property of the State.</p> <p>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.</p> <p>d. Unless otherwise stipulated, it is the State’s responsibility to identify data it deems as Non-Public Data to the Service Provider. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.</p> <p>e. At no time shall any data or processes — which either belong to or are intended for</p> | <p>the right places to establish whether and what type of encryption may be applied to the particular PaaS, which will vary by PaaS.</p> <p>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,</p> <p>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.</p> <p>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</p> | <p>Deleted “b”- Already covered in #2</p> <p>d. Encryption of Data at Rest: Where provided as part of the services, 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.</p> <p>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.e. Unless otherwise stipulated,. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.</p> <p>At no time shall any State data or processes — 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.</p> | | | <p>and options, but this generally would not be part of the contract.</p> <p>IaaS:</p> <p>For IaaS, safeguarding the confidentiality, integrity and availability of State information is subject to the State’s control, not the Contractor’s control. The State implements the controls that are available to it as features of IaaS.</p> <p>a.1 should read “The California Information Practices Act (Civil Code Sections 1798 et seq) applicable to Service Provider as a provider of IaaS”</p> <p>a. 2 should read: “Service Provider provides physical security measures for computing environments hosting Cloud Services in accordance with the NIST 800-53 framework.”</p> <p>a. 3 should read: “Privacy provisions of the Federal Privacy Act of 1974 applicable to Service Provider as a provider of IaaS and only to the extent required by a U.S. governmental agency for this scope of services.”</p> <p>3. c Encryption available in</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|---|---|--|---|---|
| <p>must be stored on a Service Provider portable device in order to accomplish work as defined in the SOW and/or SLA.</p> <p>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.</p> <p>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 Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State.</p> | <p>the use of State or its officers, agents or employees — be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State.</p> | <p>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.</p> <p>Comment: As written in the template the provision could extend to the Service Provider’s own data, and prevent the Service Provider from delivering the service as intended – storing data, backing it up, providing support, etc. – without express written consent for every normal service function.</p> | <p>The Service Provider should not use State Data or processes without written consent.</p> | | | <p>IaaS is the responsibility of the State. The user of IaaS is responsible for encryption and access control.</p> <p>3. d Customers will be informed of encryption levels and options, but this generally would not be part of the contract.</p> |
| <p>4. Data Location:</p> <p>The Service Provider shall provide its services to the</p> | <p>4. Data Location:</p> <p>The Service Provider shall provide its services to the</p> | <p>No Comment</p> | <p>No Comment</p> | <p>Unless otherwise specified in the SOW. The Contractor shall ensure the Service Provider provides its services to the State and its end users</p> | <p>IaaS: ...provide technical support, or as necessary for the delivery of the services to the State</p> | <p>PaaS/IaaS: Data centers are located globally. However, if the State wants to use data centers</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|----------------------------|-----|--|-------------------------------|---|
| <p>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.</p> | <p>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.</p> | | | <p>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 Contractor shall ensure the Service Provider 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 shall permit its personnel, and contractors to access State Data remotely only as required to provide technical or customer 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.</p> <p>Continental United States -This may eliminate some service providers.</p> <p>In the event our company has to access data, it would be for customer support, not technical. The actual service provider, as our sub, would need access for tech support.</p> <p>Not all providers may offer the same support, so we can break</p> | <p>and/or maintenance....</p> | <p>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.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|---|---|--|---|--|
| | | | | down by SOW for specific products. | | |
| <p>5.Security Incident Or Data Breach Notification:</p> <p>The 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.</p> <p>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</p> | <p>5.Security Incident Or Data Breach Notification:</p> <p>The Service Provider shall inform the State of any Security Incident or Data Breach related to State Data within the possession or control of the Service Provider and related to the service provided under this Contract.</p> <p>a. Security Incident Reporting Requirements: 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.</p> <p>b. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed Data Breach that affects the security of any State Data</p> | <p>The Contractor 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.</p> <p>b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall promptly, but in no event in more than 48 hours, after becoming aware of a Security Incident report such Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA.</p> <p>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 48 hours or sooner</p> | <p>The Service Provider shall inform the State of any Data Breach within the possession and control of the Service Provider and related to service provided under this Contract.</p> <p>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.</p> <p>Deleted a, b, c</p> <p>Breach Reporting Requirements: If the Service Provider has actual knowledge of a 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</p> | <p>The Contractor shall ensure the Service Provider informs the State of any Security Incident.....</p> <p>b. Unless otherwise stipulated, the Contractor shall ensure the Service Provider immediately reports a Security Incident.....</p> <p>c.the Contractor shall ensure the Service Provider (1) promptly 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.</p> | <p>IaaS: Unless otherwise stipulated in the SOW and/or SLA, the Service Provider shall inform the State of any Security Incident or Data Breach related to State Data within the possession or control of the Service Provider and related to the service provided under this Contract.</p> <p>Comment: This accounts for the identical qualifier in 5(a)</p> <p>a. Security Incident Reporting Requirements: Unless otherwise stipulated in the SOW and/or SLA, the Service Provider shall immediately report a Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA.</p> <p>Comment for a: A "Service Health Dashboard" (http://status.aws.amazon.com/) is available and maintained by the customer</p> | <p>PaaS:</p> <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 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.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|----------------------------|---|-----|---|---|
| <p>Contract.</p> <p>b. Security Incident Reporting Requirements: 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.</p> <p>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 24 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.</p> | <p>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, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.</p> | | <p>notify the appropriate State Identified Contact , and (2) take commercially reasonable measures to address the Data Breach in a timely manner.</p> | | <p>support team to alert customers to any issues that may be of broad impact.</p> <p>b. Breach Reporting Requirements: Unless otherwise stipulated in the SOW and/or SLA, if the Service Provider has actual knowledge of a confirmed Data Breach of security measures required by this Contract that affects the security of any State Data that is subject to applicable Data Breach notification law, the Service Provider shall (1) promptly notify</p> <p>The State within 48 hours after the Service Provider confirms the Data Breach, unless shorter time is required by applicable law, and unless prior notification is prohibited by court order or other legal requirement, and (2)....</p> <p>Comments:</p> <p>Custom notice recipients are typically very difficult for a scalable organization such as an IaaS provider to adhere</p> | <p>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>IaaS:</p> <p>Entire Section 5: Flexibility is required. This section should be preceded with “Unless otherwise described in a</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|------|------|----------------------------|-----|-----|--|--|
| | | | | | <p>to, especially given the very short timeframe in this provision. 48 hours is a more reasonable period for notification.</p> | <p>Service Description or Statement of Work...”</p> <p>5.a Most of IaaS offerings are unmanaged services, meaning these are managed by the customer, not the Service Provider. IBM can agree to provide notification of Security Incidents of which it is are, but the State, in an unmanaged environment, may become aware of a Security Incident before Service Provider is, in which case the State should notify Service Provider. “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 IaaS customers at the same time. We cannot accommodate a different notice</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|--|--|--|---|---|
| | | | | | | <p>schedule for individual customers.</p> <p>5.b See comments above for 5.b. Not all measures may apply to PaaS. Flexibility is required to adapt these terms to the particular offering.</p> |
| <p>6. Data Breach Responsibilities: 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.</p> <p>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.</p> <p>b. The Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall</p> | <p>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.</p> <p>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.</p> <p>b. The Service Provider, unless stipulated otherwise in the</p> | <p>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, 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.</p> <p>c. Service Provider will provide 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, regarding findings and actions performed by Service Provider to the State Identified Contact until the</p> | <p>Deleted sections a, c & d.</p> <p>The Service Provider, unless stipulated otherwise in the SOW and/or SLA, shall promptly notify the appropriate State Identified Contact, , if it confirms 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 , if necessary.</p> <p>Prompt notice should be sufficient.</p> <p>This should be limited to confirmed breaches</p> | <p>a. The Contractor shall ensure the Service Provider, unless stipulated otherwise in the SOW and/or SLA , immediately 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.</p> <p>b. The Contractor shall ensure the Service Provider, unless stipulated otherwise in the SOW and/or SLA, promptly 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 (1) cooperates with</p> | <p>IaaS:</p> <p>Deleted sections a and c.</p> <p>b. TheThe 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) conduct a post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.</p> <p>e. Unless otherwise stipulated in the SOW and/or SLA, if the Service Provider is required by the Contract to encrypt Personal Data and/or Non-Public Data and a Data Breach is a direct result of that obligation, the Service Provider.....</p> | <p>PaaS/IaaS:</p> <p>PaaS/IaaS 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 “Security Incident”), such party will promptly (and no more than required under applicable law, to the extent that any such law applies to notifications between a Service Provider and State) notify the other party of such Security Incident in writing (e.g., via email) upon becoming aware thereof and provide sufficient details to enable Service Provider to identify the (suspected) breach and the notified party will provide reasonable assistance to</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|--|--|---|---|-----------------------|---|
| <p>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.</p> <p>c. Service Provider will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service Provider to the State Identified Contact until the</p> | <p>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.</p> <p>c. Service Provider will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service</p> | <p>Data Breach has been effectively resolved to the State’s satisfaction.</p> <p>Comments: It is impractical and unnecessary for Service Providers to generically commit to daily, or more frequent updates. Situations of this type are fluid and PaaS providers have thousands or millions of customers who may also be affected by the Security Incident or Data Breach, who may be affected in different ways. The State is best served by the Service Provider focusing on fixing the problem, and updating the State and other customers at the time of important developments.</p> <p>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 prevent its release, the Service Provider shall bear the costs associated with (1) its investigation</p> | <p>The State may have to change business practices</p> <p>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 contractual obligation to encrypt Personal Data and/or Non-Public Data, 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.</p> | <p>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....</p> <p>c. The Contractor shall ensure Service Provider provides weekly updates, or more frequently if 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.</p> <p>d. The Contractor shall ensure Service Provider quarantine the Data Breach, ensures secure access to Data, and repair....</p> <p>e. Service Provider’s breach of its obligation to encrypt Personal Data and/or Non-Public Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2)</p> | | <p>conduct a review of the same. 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 of Contact. 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> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|--|----------------------------|-----|--|-----------------------|-----|
| <p>Data Breach has been effectively resolved to the State’s satisfaction.</p> <p>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.</p> <p>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 otherwise prevent its release, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State (or</p> | <p>Provider to the State Identified Contact until the Data Breach has been effectively resolved to the State’s satisfaction.</p> <p>d. Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair IaaS as needed in accordance with the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.</p> <p>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 otherwise prevent its release, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals,</p> | | | <p>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</p> | | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|--|--|---|---|--------------------------|
| <p>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.</p> | <p>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.</p> | | | | | |
| <p>7. Notification of Legal Requests 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</p> | <p>7. Notification of Legal Requests: 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</p> | <p>To the extent legally permitted, 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, which in any way will 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</p> | <p>Unless otherwise required by law, the Service Provider shall contact the State upon receipt of any electronic discovery,</p> | <p>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 respond to subpoenas, service of</p> | <p>IaaS:</p> <p>other legal requests related to the State without first notifying the State (unless prohibited by law from providing such notice),</p> <p>with adequate time for the State to</p> <p>seek a protective order in a court of competent jurisdiction if necessary.</p> | <p>No Comment</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|--|--|---|--|--|--|
| <p>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.</p> | <p>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.</p> | <p>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, 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 (as opposed to Service Provider) unless authorized in writing to do so by the State.</p> <p>Comment: Service Providers can provide notice to the State of any compelled legal process as permitted by law, but it cannot permit the State a unilateral right to revise responses to the compelled legal process. The Service Provider to whom a compelled legal process has been directed must have control over its response to that process.</p> | | <p>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, agree 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 respond to legal requests</p> | | |
| <p>8. Data Preservation and Retrieval:</p> <p>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</p> | <p>8. Data Preservation and Retrieval:</p> <p>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</p> | <p>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 the State for extracting and/or transitioning, all State</p> | <p>Delete section d.</p> <p>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.</p> | <p>b. The Contractor agrees to</p> <p>f. During any period of suspension, the Contractor shall, and ensure the Service Provider</p> <p>g. The Contractor will impose no fees</p> | <p>IaaS: Delete sections c and g.</p> <p>a. For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Service Provider shall make the services available for the State to extract and/or transition all</p> | <p>PaaS: 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</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|---|--|--|--|---|
| <p>transitioning all State Data in the format determined by the State (“Transition Period”).</p> <p>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.</p> <p>c. During the Transition Period, PaaS and State Data access shall continue to be made available to the State without alteration.</p> <p>d. Service Provider agrees to compensate the State for damages or losses the State incurs as a result of Service Provider’s failure to comply with this section in accordance with the “Limitation of Liability” provision set forth in the General Provisions - Information Technology.</p> <p>e. The State at its option, may purchase additional transition services as agreed upon in the SOW and/or SLA.</p> <p>f. During any period of suspension, the Service</p> | <p>and/or transitioning all State Data in the format determined by the State (“Transition Period”).</p> <p>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.</p> <p>c. During the Transition Period, IaaS and State Data access shall continue to be made available to the State without alteration.</p> <p>d. Service Provider agrees to compensate the State for damages or losses the State incurs as a result of Service Provider’s failure to comply with this section in accordance with the “Limitation of Liability” provision set forth in the General Provisions - Information Technology.</p> <p>e. The State at its option, may purchase additional transition services as agreed upon in the SOW and/or SLA.</p> | <p>Data in the commonly used format by the Service Provider (“Transition Period”).</p> <p>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.</p> <p>g. The Service Provider will impose no fees for normal access and retrieval of digital content to the State.</p> <p>h. After termination of the Contract and the prescribed retention period, 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.</p> | <p>g. The Service Provider will impose no additional fees for access and retrieval of Data by the State.</p> <p>h. After termination of the Contract and any prescribed retention period...</p> | <p>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, and paper.</p> | <p>State Data in the format determined by the State (“Transition Period”).</p> <p>d. Service Provider agrees to compensate the State for damages or losses the State incurs as a result of Service Provider’s failure to comply with this section in accordance with the “Limitation of Liability” provision set forth in the General Provisions - Information Technology.</p> <p>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. Infrastructure components shall be permanently deleted according to NIST-approved methods. Certificates of destruction shall be provided to the State.</p> | <p>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>IaaS: Under the self-managed approach the State migrates data in and is responsible to migrate out. If State requires assistance from Service Provider, such assistance must be contracted for as additional migration /managed services. Format may vary depending upon offering. IBM may charge for certain transition activities such as delivering content in a specific format. a.b. and c. need to be modified to reflect the above requirements.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|--|---|---|---|--|
| <p>Provider shall not take any action to intentionally erase any State Data.</p> <p>g. The Service Provider will impose no fees for access and retrieval of digital content to the State.</p> <p>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. Certificates of destruction shall be provided to the State.</p> | <p>f. During any period of suspension, the Service Provider shall not take any action to intentionally erase any State Data.</p> <p>g. The Service Provider will impose no fees for access and retrieval of digital content to the State.</p> <p>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. Certificates of destruction shall be provided to the State.</p> | | | | | |
| <p>9. Background Checks: As permitted by law, the Service Provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to</p> | <p>9. Background Checks: As permitted by law, the Service Provider shall conduct criminal background checks and not utilize any staff, including</p> | <p>As permitted by law, the Service Provider shall conduct criminal background checks and not knowingly permit any staff, including subcontractors, to have logical access to Personal Data and Non-</p> | <p>...up to 1 year is an authorized penalty within the past five years. The Service Provider Added standard background check time period</p> | <p>As permitted by law, the Contractor shall ensure the Service Provider conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the services who have</p> | <p>IaaS: “to fulfill the obligations of the Contract”</p> | <p>PaaS Replace 9 with: When required under a Statement of Work, and at the State’s expense, the Service Provider shall conduct a background investigation in</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|---|--|--|--|--|
| <p>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.</p> | <p>subcontractors, to fulfill the obligations of the Contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. 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.</p> | <p>Public Data who have been convicted of any crime of dishonesty, including but not limited to criminal fraud.</p> | | <p>been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall, and ensure the Service Provider shall, promote and maintain an awareness of the importance of securing the State's information among their respective employees and agents.</p> | | <p>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>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 latency statistics, user access, user access IP address, user access history and security logs for all State files related to this Contract.</p> | <p>10. Access To Security Logs And Reports:</p> <p>a. The Service Provider shall provide reports to the State directly related to the infrastructure the Service Provider controls upon which the State account resides. Unless otherwise agreed to in the SLA, the Service Provider shall provide the State a history of all Application Program Interface (API) calls for the</p> | <p>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</p> <p>Comment:</p> <p>The details may vary by PaaS and so is most appropriate in the SOW.</p> | <p>As described in the SOW or SLA, 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 as part of the services, reports will include latency statistics</p> | <p>a. The Contractor shall ensure the Service Provider provides reports to the State in a format as specified in the SOW and/or SLA....</p> <p>b. The Contractor and the State recognize that security responsibilities are shared. The Contractor is responsible for ensuring the Service Provider provides a secure infrastructure.</p> | <p>IaaS comment:</p> <p>Log reports are frequently available as a service feature. It should be made clear that either (1) the Service Provider should provide these reports, or (2) similar reports must be available on the services.</p> | <p>PaaS:</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.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|---|--|--|--------------------------|--|
| <p>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.</p> | <p>State account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Service Provider. The report will be sufficient to enable the State to perform security analysis, resource change tracking and compliance auditing.</p> <p>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.</p> | | | | | <p>This must be addressed in a SOW.</p> <p>IaaS:</p> <p>This section is not entirely accurate. IaaS provides State with the ability to “self-manage”, meaning create, monitor and store logs by itself. A Cloud Manage Service Delivery model provides limited reference to security logs. Depending upon Service Options chosen for i.e. HIPAA, PCI, etc. may have enhanced capability to create, monitor and store logs. This must be addressed in a SOW.</p> |
| <p>11. Contract Audit: The Service Provider shall allow the State to audit</p> | <p>11. Contract Audit: The Service Provider shall allow the State to audit</p> | <p>Upon request the Service Provider will make available to the State copies or summaries of its regularly</p> | <p>The Service Provider shall allow the State reasonable access to audit conformance to the Contract terms no more</p> | <p>The Contractor shall allow the State to audit Contractor’s and Service Provider’s conformance to the Contract</p> | <p>No Comment</p> | <p>No Comment</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|---|---|---|-----------------------------|--|
| 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. | 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. | 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. | than once annually. 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. | terms, provided the parties first agree to the scope, timing, duration and expectations of the audit. | | |
| 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 | 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 | 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 | Added 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 month's | The Contractor shall ensure the Service Provider 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 no cost to the State. The Contractor shall provide a redacted version of the Service Provider's audit report and its plan to correct any negative findings... | IaaS: "redacted version" | Section 12 needs additional details and clarification. IBM recommends the following: Service Provider will arrange for the performance of audits and production of an audit report by an independent third party in accordance with the most recent "Service Organizational Control Type II Report" made in accordance with Statements on Standards for Attestation Engagements No. 16 ("SOC2 Report") |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|--|--|--|--|---|
| to correct any negative findings upon request. The Service Provider may remove its proprietary information from the redacted version. | Contractor's plan to correct any negative findings upon request. The Service Provider may remove its proprietary information from the redacted version. | remove its proprietary information from the redacted version. | advanced notice and the State may terminate the services with 30 days written notice and without paying a termination charge. | | | 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: 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 ware with a newer or better version in order to bring the system up to date or to | 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 ware with a newer or better version in order to bring the system up to date | 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 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. Comment: | | The Contractor shall ensure the Service Provider give advance notice... | IaaS: The Service Provider shall give advance notice to the extent agreed to by the parties | This depends on the service and must be mutually agreed in a SOW. |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|--|---|---|--|---|
| improve its characteristics. It usually includes a new version number. | or to improve its characteristics. It usually includes a new version number. | As originally written it would sweep up all of the daily running of the PaaS, whether the impact was significant or insignificant, positive or negative. | | | | |
| 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. | 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. | | | The Contractor shall, and ensure the Service Provider shall, disclose 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 Contractor shall understand each other's, and the Service Provider's , roles and responsibilities..... | IaaS: "such that adequate protection and flexibility can be attained between the State and the Service Provider" | 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: The Service Provider shall enforce separation of job duties; require commercially reasonable non-disclosure agreements, including those that may be required by the State, and limit staff knowledge of State Data to that which is absolutely necessary to perform job | 15. Non-Disclosure and Separation of Duties: The Service Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, including those that may be required by the State, and limit staff knowledge of State Data to that which is absolutely necessary to perform job | 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 to perform job duties. Comment : It's not in the interest of PaaS | The Service Provider shall enforce separation of job duties,, and limit staff knowledge of State Data to that which is necessary to perform job duties. | The Contractor shall enforce separation of job duties | IaaS: Deleted Section 15 Such infrastructure access controls should be the subject of the SLA and/or SOW | This provision is unclear. More information regarding the intent is requested. |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|---|-------------------|--|--|-------------------|
| duties. | duties. | customers (including the State) to try to restrict this to absolutes. For example, it is arguably not "absolutely necessary" for a product developer to know how the State is using the PaaS but without that knowledge it is difficult for the Service Provider to take the State's wishes and objectives into account in its product development. | | | | |
| 16. Import and Export of Data: The State shall have the ability to import or export data in whole or in part at its discretion without interference from the Service Provider. This includes the ability for the State to import or export data to or from other Service Providers. | 16.Import and Export of Data: The State shall have the ability to import or export data in whole or in part at its discretion without interference from the Service Provider. This includes the ability for the State to import or export data to or from other Service Providers. | 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. | No Comment | The State 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. | No Comment | No Comment |
| 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, | 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, | The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support necessary to provide the PaaS services in accordance with this Contract and the SOW. The technical and professional activities required for establishing, | No Comment | The Contractor shall be Responsible..... | The system shall be available 24/7/365 (with agreed-upon maintenance downtime), subject to the limitations and any remedies provided for in the SOW and/or SLA. | No Comment |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|--|--|--------------------------|--|--------------------------|--------------------------|
| <p>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.</p> | <p>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.</p> | <p>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</p> <p>24/7/365 (with agreed-upon maintenance downtime), and shall provide service to customers as defined in the SOW and/or SLA.</p> <p>Comment: Service Providers can discuss more detailed SLAs in the SOW or SLA attachment, but the template language reflects 100% availability (other than planned downtime), which is not achievable by anyone running an IT system.</p> | | | | |
| <p>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</p> | <p>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</p> | <p>Deleted section 18.</p> | <p>No Comment</p> | <p>The 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</p> | <p>No Comment</p> | <p>No Comment</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|--|--------------------------|---|--------------------------|--|
| 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. | 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. | | | similar agreement with the Contractor, | | |
| <p>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.</p> | <p>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</p> | <p>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 security violation exists with respect to the request, the Service Provider shall promptly 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.</p> <p>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</p> | <p>No Comment</p> | <p>The State shall have the right at any time to request the Contractor remove from Interaction with State any Contractor or Service Provider representative who the State believes is detrimental to its working relationship with the Contractor. The State shall provide the 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 determines in its reasonable discretion that the potential violation is valid, the Contractor shall immediately remove such individual. The Contractor shall not assign the person...</p> | <p>No Comment</p> | <p>Delete as these are individuals that are supporting multiple IaaS/PaaS accounts and individuals may be critical to support.</p> <p>A better approach would be for the State to raise concerns to Service Provider to address and discuss appropriate measures with the State.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|--|--|---|--|---|--|
| | orders without the State's consent. | <p>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.</p> <p>Comment:</p> <p>This type of clause is appropriate in a professional services agreement, where services are being provided uniquely and directly to a particular customer. It does not work in a PaaS agreement where employees are servicing thousands or millions of customers. To the extent a Service Provider staff person visits the State's facilities or is dedicated exclusively to providing the services to the State, Service Provider can accept the clause as edited.</p> | | | | |
| <p>20. Business Continuity and Disaster Recovery: The Service Provider shall provide a business continuity and disaster recovery plan upon request and shall ensure that it achieves the State's</p> | <p>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</p> | <p>The Service Provider shall provide a business continuity and disaster recovery plan upon request which reflects the Recovery Time Objective (RTO), agreed to by the parties and set forth in the SOW and/or SLA.</p> | <p>To the extent available as part of the services, the Service Provider shall provide...</p> <p>In the notification, to the extent possible, Service</p> | <p>The BC/DR would apply to our services, which don't include the actual hosted services. The State probably would want to see the service provider's plans, so we would reflect the language that we would ensure the SP does this.</p> | <p>IaaS:</p> <p>Kept introduction but Deleted a, b, c.</p> | <p>This section should be deleted or should reference the capabilities that are predefined in the standard products. For IaaS, these services are not customized for individual customers. It is the state's responsibility to determine</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|--|---|--|-----------------------|--|
| <p>Recovery Time Objective (RTO), as agreed to by the parties and set forth in the SOW and/or SLA.</p> <p>a. In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to State Data, Service Provider shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the Contracting agency. Service Provider shall provide such notification within twenty-four (24) hours after Service Provider reasonably believes there has been such a disaster or catastrophic failure. In the notification, Service Provider shall inform the State of:</p> <p>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</p> | <p>achieves the State’s Recovery Time Objective (RTO), as agreed to by the parties and set forth in the SOW and/or SLA.</p> <p>a. In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to State Data, Service Provider shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the Contracting agency. Service Provider shall provide such notification within twenty-four (24) hours after Service Provider reasonably believes there has been such a disaster or catastrophic failure. In the notification, Service Provider shall inform the State of:</p> <p>i. The scale and quantity of the State Data loss; ii. What Service Provider has done or will do to</p> | <p>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 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 (48) 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:</p> | <p>Provider shall inform the ...</p> <p>Delete section a iv</p> <p>Delete from b:</p> | <p>The Contractor shall ensure the Service Provider provides a business continuity...</p> <p>a. .. loss of access to State Data, the Contractor shall ensure the Service Provider notifies 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. The Contractor shall ensure the Service Provider 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 informs the State...</p> <p>b. The Contractor shall ensure Service Provider restores continuity of.....</p> <p>c. The Contractor shall ensure the Service Provider 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</p> | | <p>whether the predefined RTO meets their requirements.</p> <p>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.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|---|---|----------------------------|-----|--|-----------------------|-----|
| <p>any deleterious effect of the State Data loss; and</p> <p>iii. What corrective action Service Provider has taken or will take to prevent future Data loss.</p> <p>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.</p> <p>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 may result in the State exercising its options for assessing damages or other remedies under this Contract.</p> <p>c. Service Provider shall conduct an investigation of the disaster or catastrophic</p> | <p>recover the State Data and mitigate any deleterious effect of the State Data loss; and</p> <p>iii. What corrective action Service Provider has taken or will take to prevent future Data loss.</p> <p>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.</p> <p>b. Service Provider shall restore continuity of IaaS, restore State Data in accordance with the RTO as set forth in the SOW and/or SLA, restore accessibility of State Data, and repair IaaS as needed to meet the performance requirements stated in the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.</p> | | | <p>lead (if required by law) or participate in the investigation. The Contractor shall ensure the Service Provider cooperates fully with the State...</p> | | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS | IaaS | Sales Force (PaaS Only) | HPE | SHI | Amazon (IaaS Only) | IBM |
|--|---|---|---|---|--|------------|
| 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. | 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. | No corresponding clause – not relevant to service model. Standards would be selected by the State. | 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. | No Comment | The Contractor shall ensure the Service Provider complies with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973. | No Comment | No Comment |
| 22. Web Services: The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible. | 22. Web Services: The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible. | | The Service Provider shall use Web services to interface with State Data in near real time when possible. | The Contractor shall ensure the Service Provider uses Web services exclusively to interface with State Data in near real time when possible. | IaaS: Kept introduction but Deleted a, b, c. | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS and IaaS General Comments | | | | |
|---|---|---|---|---|
| EDD PaaS and IaaS | HPE PaaS suggested sections | HPE IaaS suggested sections | Internet Association | IBM Suggested Changes to IT General Provisions |
| <p>Recommend some mention regarding monitoring in general or monitoring unauthorized access. Various forms to consider, but these may be more specialized depending on the data classification: Performance, security, access... Egress (e.g. how we get out of the cloud once we are in) is a big area that should have a little more meat in it.</p> <p>For example. If SLA's X, Y, or Z do not meet SLA's 3 months in a row, the state can exercise an Out clause and egress costs will be the responsibility of the Cloud provider....</p> <p>SLA's and associated penalties if they are not met. This is the primary way to ensure that the vendor has a monthly WIFM to ensure the SLA's are met.</p> <p>PLEASE: Change the font as the current one is very hard on the eyes.</p> | <p>23. LIMITED USE: 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.</p> <p>24. ORDERING: "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.</p> <p style="padding-left: 20px;">a. Contract order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.</p> <p style="padding-left: 20px;">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.</p> | <p>21. LIMITED USE: 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.</p> <p>22. ORDERING: "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.</p> <p style="padding-left: 20px;">a. Contract order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.</p> <p style="padding-left: 20px;">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.</p> | <p>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.</p> <p>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</p> <p>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.</p> <p>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</p> | <p>General Provisions - IT: 16. Inspection, Acceptance and Rejection Inspection, Acceptance and Rejection does not apply to IaaS. Once the customer purchases IaaS, the service begins. There is no ability to reject the service, other than as part of the termination provisions that accompany the service.</p> <p>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).</p> <p>General Provisions – IT: 46. Examination and Audit The records that will be made available to the State will only be those that document the State's usage of the IaaS. Records relating to multi-tenant usage will not be made available, due to confidentiality concerns.</p> |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS and IaaS General Comments | | | | |
|---------------------------------------|---|---|---|---|
| EDD PaaS and IaaS | HPE PaaS suggested sections | HPE IaaS suggested sections | Internet Association | IBM Suggested Changes to IT General Provisions |
| | <p>e. Orders may be placed consistent with the terms of this Contract during the term of the Contract.</p> <p>f. All Orders pursuant to this Contract, at a minimum, shall include:</p> <ol style="list-style-type: none"> (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). <p>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.</p> <p>h. Orders must be placed pursuant to this Contract before the termination date of</p> | <p>e. Orders may be placed consistent with the terms of this Contract during the term of the Contract.</p> <p>f. All Orders pursuant to this Contract, at a minimum, shall include:</p> <ol style="list-style-type: none"> (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). <p>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.</p> <p>h. Orders must be placed pursuant to this Contract before the termination date of</p> | <p>services:</p> <p>The United States Navy's "Cloud Store"</p> <ul style="list-style-type: none"> • 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. <p>The Canadian Government Embraces the Cloud</p> <ul style="list-style-type: none"> • 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. <p>California's New Child Welfare System</p> <ul style="list-style-type: none"> • 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. | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS and IaaS General Comments | | | | |
|---------------------------------------|---|---|---|---|
| EDD PaaS and IaaS | HPE PaaS suggested sections | HPE IaaS suggested sections | Internet Association | IBM Suggested Changes to IT General Provisions |
| | <p>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.</p> <p>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.</p> <p>25. TITLE TO PRODUCT: 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</p> | <p>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.</p> <p>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.</p> <p>23. TITLE TO PRODUCT: 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</p> | <p>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:</p> <p>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.</p> | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS and IaaS General Comments | | | | |
|---------------------------------------|--|--|---|---|
| EDD PaaS and IaaS | HPE PaaS suggested sections | HPE IaaS suggested sections | Internet Association | IBM Suggested Changes to IT General Provisions |
| | <p>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.</p> <p>26. 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.</p> <p>27. CHANGE ORDERS: 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.</p> <p>28. 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 Service Provider, and provide whatever</p> | <p>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.</p> <p>24. 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.</p> <p>25. CHANGE ORDERS: 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.</p> <p>26. 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 Service Provider, and provide whatever</p> | <p>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.</p> <p>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</p> | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS and IaaS General Comments | | | | |
|--------------------------------|--|--|--|--|
| EDD PaaS and IaaS | HPE PaaS suggested sections | HPE IaaS suggested sections | Internet Association | IBM Suggested Changes to IT General Provisions |
| | <p>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.</p> <p>29. GLOBAL TRADE COMPLIANCE: 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.</p> | <p>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.</p> <p>27. GLOBAL TRADE COMPLIANCE: 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.</p> | <p>customary commercial practice.</p> <p>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.</p> <p>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.</p> <p>4. Security, privacy and audit–The key to contracting for and analyzing security,</p> | |

Cloud As-A-Service

Clause Comparison Matrix

| PaaS and IaaS General Comments | | | | |
|---------------------------------------|------------------------------------|------------------------------------|--|---|
| EDD PaaS and IaaS | HPE PaaS suggested sections | HPE IaaS suggested sections | Internet Association | IBM Suggested Changes to IT General Provisions |
| | | | <p>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.</p> <p>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.</p> <p>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.</p> | |