STATE OF IDAHO STANDARD TERMS AND CONDITIONS FOR CLOUD SERVICES

Note: In the event of conflict with the State of Idaho Standard Contract Terms and Conditions, the following provisions will take precedence:

1. DEFINITIONS: Unless the context clearly requires otherwise, the definitions set forth in the *State of Idaho Standard Contract Terms and Conditions* shall apply to terms used in these *State of Idaho Standard Terms and Conditions for Cloud Services*. In addition, the following terms shall have the following meanings when used in these *State of Idaho Standard Terms and Conditions for Cloud Services*:

A. Data Breach - Any unauthorized access to or acquisition of Non-Public State Data following a Security Incident that compromises the security, confidentiality, or integrity of the Non-Public State Data, or the ability of the State to access the Non-Public State Data.

B. Infrastructure as a Service (IaaS) - The capability provided to the user to provision processing, storage, networks, and other fundamental computing resources where the user is able to deploy and run arbitrary software, which can include operating systems and applications. The user does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

C. Non-Public State Data - State 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, ordinance or administrative rule from access by the general public as public information. Non-Public State Data includes, but is not limited to, Personal State Data.

D. Personal State Data - State Data alone or in combination with other data that includes information relating to an individual that identifies the individual by name, identifying number, mark or description that can be readily associated with a particular individual and which is not a public record. Personal State Data includes but is not limited to 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; Protected Health Information (PHI) relating to a person; or 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).

E. Platform as a Service (PaaS) - The capability provided to the user to deploy onto the cloud infrastructure user-created or user-acquired applications created using programming languages and tools provided by the Contractor. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

F. Protected Health Information (PHI) - Individually identifiable health information held or transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI also includes but may not be limited to 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.

G. Service – The performance of the specifications and requirements described in the Contract.

H. Security Incident - The unauthorized access to the Contractor's network that the Contractor or the State believes could reasonably result in the use, disclosure or theft of the State's Non-Public State Data within the possession or control of the Contractor. A Security Incident also includes a security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to the State's Non-Public State Data. A Security Incident may or may not turn into a Data Breach.

I. Software as a Service (SaaS) - The capability provided to the user to use the Contractor's applications running on the Contractor's infrastructure (commonly referred to as "cloud infrastructure"). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

J. State Data - All information and data developed, documented, derived, stored, installed or furnished by the State under the Contract, including all data related to records owned by the State of Idaho.

K. Update – An enhancement, repair, patch or fix to a Service.

L. FedRAMP – Federal Risk and Authorization Management Program; a civilian-side, federal government-wide program that standardizes the approach to assessing, authorizing and continuously monitoring cloud products and services: https://www.fedramp.gov/.

2. Subscription Terms: Contractor grants to the State a license to: (i) access and use the Service for its business purposes; (ii) use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

3. Data Access Controls: Contractor will provide access to State Data only to those Contractor employees and subcontractors ("Contractor Staff") who need to access the State Data to fulfill Contractor's obligations under the Contract. Contractor shall not allow access the State's user accounts or State Data, except during the course of data center operations, in response to service or technical issues, as required by the express terms of these *State of Idaho Standard Terms and Conditions for Cloud Services*, or at the State's written request. Contractor must not share State Data with its affiliates or any third party without the State's express written consent. Contractor must ensure that, prior to being granted access to the State Data, Contractor Staff who perform work under the Contract have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all State Data protection provisions of the Contract, and that Contractor Staff possess qualifications appropriate to the nature of the employees' duties and the sensitivity of the State Data they will be handling.

4. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Service in a manner that is, at all times during the term of the Contract, at a level equal to or more stringent than those specified in the Contract.

5. Data Ownership: The State owns and retains full right and title, and unrestricted access to State Data. Additionally, the State retains the right to back-up State Data at its own data center. Contractor shall not collect, access, or use State Data except (1) in the course of data center operations pursuant to Service provided under this Contract, (2) in response to service or technical issues, (3) as required or expressly allowed by the terms of the Contract, or (4) at the State's written request. Except as expressly allowed by the terms of the Contract, no information regarding the State's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. These obligations shall extend beyond the term of the Contract in perpetuity.

6. Service Failure or Damage: In the event of Service failure or damage caused by Contractor or its Service, the Contractor agrees to restore the Service within twenty-four (24) hours after failure or damage is sustained, unless otherwise specified in the Contract, or agreed to in writing by the State.

7. Title to Product: If access to the Service requires an application program interface (API), Contractor shall convey to the State an irrevocable and perpetual license to use the API for the duration of the Contract.

8. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, specific to the type(s) of Data and as otherwise specified in the Contract, which may include, but is not limited to IRS Pub 1075, HIPAA, PCI, and FERPA.

9. Warranty: In addition to any other requirements for warranties elsewhere in the Contract, the Contractor warrants the following:

A. Contractor has acquired all rights for the Contractor to provide the Service described in the Contract.

B. Contractor will perform materially as described in the Contract.

C. That the Service is fit for a particular purpose.

D. The Contractor will not interfere with the State's access to and use of the Service it acquires under the Contract.

E. The Service(s) provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified in the Contract.

F. The Service it provides under the Contract is free of malware, and Contractor will use for the term of the Contract current industry standard security measures to prevent from entry, detect within and remove from the Service malicious software.

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

A. All Non-Public State Data shall be encrypted at rest and in transit with controlled access. Unless otherwise provided in the Contract, the Contractor is responsible for encryption of the Non-Public State Data. All encryption shall be consistent with validated cryptography standards such as the current standards in FIPS 140-2, Security Requirements for Cryptographic Modules, or the then-current NIST recommendation.

B. The State shall identify State Data it deems as Non-Public State Data to the Contractor. The level of protection and encryption for all Non-Public State Data shall be identified in the Contract.

C. At no time shall any State Data or processes, that either belong to or are intended for the use of the State or its officers, agents or employees, be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State.

D. The Contractor shall not use any information collected in connection with the Service provided under the Contract for any purpose other than fulfilling the Service.

E. Data Location: The Contractor shall provide its Service to the State and its end users solely from data centers within the United States; and storage of State Data at rest shall be located solely in data centers within the United States. The Contractor shall not allow its personnel or subcontractors to store State Data on portable devices, except for devices that are used and kept only at its U.S. data centers. Each data center used by the Contractor to support the Contract must be within a physical security perimeter to prevent unauthorized access, and physical entry controls must be in place so that only authorized personnel have access to State Data and State-written applications.

F. The Contractor shall permit Contractor Staff to access State Data remotely only as required to provide technical support.

G. FedRAMP: State Data shall be stored in a FedRAMP accredited cloud service.

11. Shared Security Responsibilities: The Contractor and the State agree that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The State is responsible for its operating system, firewalls and other logs captured within the operating system. If there are other shared responsibilities, they must be identified within the Contract. (Note: State agencies are required to adhere to the NIST Cyber Security Framework as provided in Executive Order 2017-02.)

12. Security Incident and Data Breach Responsibilities: In the event of a Security Incident or Data Breach, the Contractor shall:

A. Notify the State-designated contact(s) by telephone within twenty-four (24 hours), unless shorter time is required by applicable law, if the Contractor has confirmed that there is, or the Contractor reasonably believes that there has been, a Security Incident or Data Breach. The Contractor shall (1) immediately quarantine all State Data from external access, (2) cooperate with the State as requested by the State to investigate and resolve the Security Incident or Data Breach, (3) promptly implement remedial measures, if necessary, (4) (for a Data Breach) identify to the State, if the following is known by the Contractor, the persons affected, their identities, and the State Data disclosed, and (5) document responsive actions taken related to the Security Incident or Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the Service, if necessary.

B. Unless otherwise stipulated in the Contract, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Non-Public State Data or otherwise prevent its release as reasonably determined by the State, the Contractor shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to by the State and the Contractor; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to by the State and the Contractor; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws; all not to exceed the average per record per person cost calculated for Data Breaches in the United States (as of January 2019, $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

C. Incident Response: The Contractor may need to communicate with outside parties regarding a Security Incident or Data Breach, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon between the State and the Contractor in writing, defined by law or contained in the Contract. Discussing Security Incidents with the State must be handled on an urgent as needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon between the State and the Contractor in writing, defined by law or as delineated in the Contract.

13. Notification of Legal Requests: The Contractor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to State Data under the Contract, or which in any way might reasonably require access to State Data. The Contractor shall not respond to subpoenas, service of process or other legal requests related to the State without first notifying and obtaining the approval of the State, unless prohibited by law from providing such notice.

14. Background Checks and Security Awareness: Upon the request of the State, the Contractor shall obtain criminal background checks for Contractor Staff that the Contractor intends to utilize in the provision of services under the Contract and must provide the results of the criminal background checks to the State. If any Contractor Staff are not acceptable to the State in its sole opinion based upon the results of a criminal background check, the State, in its sole discretion, shall have the right to request that such Contractor Staff not provide services under the Contract. The Contractor must comply with such requests and provide replacement Contractor Staff in such cases.

The Contractor shall promote and maintain an awareness of the importance of securing the State's information among the Contractor's employees and agents.

15. Data Center Audit: The Contractor shall have an independent audit of its data centers at least annually at its expense, and upon written request from the State must provide an unredacted (save that the Contractor may remove its information that is trade secret in accordance with the Idaho Public Records Act) version of the audit report to the designated State representative no later than thirty (30) calendar days after the report is published. A Service Organization Control (SOC) 2 audit report is required, or, the State may, in its sole discretion, approve another audit type upon Contractor request. In addition, the State shall have the right to inspect the data centers used by the Contractor to support the Contract, subject to reasonable restrictions imposed by Contractor, within ten (10) calendar days of written notice to Contractor, or such other timeframe as may be mutually agreed upon by the parties.

16. Change Control and Advance Notice: The Contractor shall give a minimum forty-eight (48) hour advance written notice (or as otherwise identified in the Contract) to the State of any Updates that may impact availability of Service or performance.

Contractor must provide Updates to State at no additional cost when Contractor makes such Updates generally available to its users.

No Update or other change to the Service may decrease or otherwise negatively impact the Service's functionality or adversely affect the State's use of or access to the Service.

17. Non-Disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of State Data to that which is absolutely necessary to perform job duties.

18. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the Service being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The Service shall be available twenty-four (24) hours per day, seven (7) days per week and three hundred sixty-five (365) days per year (excepting reasonable downtime for maintenance).

19. Transition, Transfer Assistance Termination or Suspension:

A. The State shall have the ability to import or export all or portions of State Data and State-written applications at its discretion without interference from the Contractor at any time during the term of the Contract. This includes the ability for the State to import or export State Data and State-written applications to and from other entities.

B. The Contractor shall reasonably cooperate without limitation with any State authorized entity for the transfer of State Data to the State upon termination or expiration of the Contract. The Contractor must transfer State Data or allow the State to extract State Data and State-written applications, at no additional cost to and in a format designated by, the State, and the State Data must be unencrypted.

C. The return of State Data and State-written applications shall occur no later than sixty (60) calendar days after termination or expiration of the Contact; or within another timeframe as agreed to in writing by the parties. Contractor shall facilitate the State's extraction of State Data and State-written applications by providing the State with all necessary access and tools for extraction, at no additional cost to the State.

D. During any period of suspension of Service, the Contractor shall continue to fulfill its obligations to maintain State Data and State-written applications.

E. In the event of termination or expiration of the Contract, the Contractor shall not take any action to intentionally erase State Data or State-written applications for a period of sixty (60) calendar days after the effective date of termination or expiration. After such period, the Contractor shall have no obligation to maintain or provide any State Data or to maintain any State-written applications and shall thereafter, unless legally prohibited, delete all State Data and State-written applications (in all forms) within its systems or otherwise in its possession or under its control, unless otherwise instructed by the State. State Data and State-written applications shall be permanently deleted and shall not be recoverable in accordance with National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the State no later than ninety (90) calendar days after termination or expiration of the Contract.

F. The Contractor must maintain the confidentiality and security of State Data and State-written applications during any transition or transfer and thereafter for as long as the Contractor possesses State Data and State-written applications.

20. Access to Security Logs and Reports: The Contractor shall provide reports to the State; or alternatively, provide the State with access to report data and reporting tools. Unless specified otherwise in the Contract, reports shall include latency statistics, system performance statistics, user access logs, user access IP address, user access history, security logs and event logs for all State Data.