TERMS AND CONDITIONS FOR CLOUD-BASED SERVICES

1. DEFINITIONS. Unless the context clearly requires otherwise, the definitions set forth in the Request for Proposals shall apply to terms used in these Terms and Conditions for Cloud Services. In addition, the following terms shall have the following meanings when used in these Terms and Conditions for Cloud-Based Services:

A. ISC Data - All information and data developed, documented, derived, stored, installed or furnished by ISC under the Contract, including all data related to records owned by ISC. ISC Data does not include end-user credit or debit card information.

B. Data Breach – Any: (1) unauthorized access to or acquisition of Non-Public ISC Data or end-user credit and debit card information following a Security Incident that compromises the confidentiality, integrity, availability, or security of the Non-Public ISC Data or end-user credit and debit card information; or (2) unauthorized access to Public ISC Data following a Security Incident that comprises the integrity, availability, or security of Public ISC Data.

C. Infrastructure as a Service (IaaS) - The capability provided to the user for 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).

D. Non-Public ISC Data - ISC Data that is not subject to distribution to the public as public information, including all information exempt from public disclosure pursuant to Idaho Court Administrative Rule 32. It is deemed to be sensitive and confidential by ISC because it contains information that is exempt by statute, ordinance, or administrative rule from access by the general public as public information. Non-Public ISC Data includes, but is not limited to, Personal ISC Data.

E. Personal ISC Data - ISC 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 ISC 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).

F. 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.

G. 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.

H. Public ISC Data – All ISC Data except Non-Public ISC Data.

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

J. Security Incident – (1) The loss of availability of a system; (2) the unauthorized access to the Contractor's network that the Contractor or ISC believes could reasonably result in the: (i) use, disclosure, alteration, destruction, or theft of Non-Public ISC Data or end-user credit and debit card information within the possession or control of the Contractor, or (ii) alteration or destruction of Public ISC Data; or (3) a security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to Non-Public ISC Data, Public ISC Data, or end-user credit and debit card information. A Security Incident may or may not turn into a Data Breach.

K. 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.

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

2. <u>Subscription Terms</u>. Contractor grants to ISC 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. <u>Data Access Controls</u>. Contractor will provide access to ISC Data and end-user credit and debit card information only to those Contractor employees and subcontractors ("Contractor Staff") who need to access ISC Data to fulfill Contractor's obligations under the Contract. Contractor shall not allow access to ISC's user accounts or ISC Data or end-user credit and debit card information, except during the course of data center operations, in response to service or technical issues, as required by the express terms of these Terms and Conditions for Cloud-Based Services, or at ISC's written request. Contractor must not share ISC Data with its affiliates or any third party without ISC's express written consent, and must not share end-user credit and debit card information with its affiliates or any third party except to the extent necessary to provide the Service. Contractor must ensure that, prior to being granted access to ISC Data or end-user credit and debit card information, 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 ISC Data and end-user credit and debit card information protection provisions

of the Contract, and that Contractor Staff possess qualifications appropriate to the nature of the employees' duties and the sensitivity of ISC Data and end-user credit and debit card information they will be handling. This includes but is not limited to annual, role-based security awareness training.

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 and Availability. ISC owns and retains full right and title, and unrestricted access to and right to copy ISC Data. Additionally, ISC retains the right to back-up ISC Data at its own data center. Contractor shall not collect, access, or use ISC 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 ISC's written request. Except as expressly allowed by the terms of the Contract, no information regarding ISC'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 ISC.

7. Title to Product. If access to the Service requires an application program interface (API), Contractor shall convey to ISC 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, rules and regulations 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 Idaho Court Administrative Rule (ICAR) 32, FBI's Criminal Justice Information Services (CJIS) Compliance, IRS Publication 1075, Health Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) security standards, Driver's Privacy Protection Act (DPPA), and Family Education Rights Privacy Act (FERPA).

9. Warranty. In addition to any other requirements for warranties elsewhere in the Contract, the Contractor warrants the following: (i). Contractor has acquired all rights for the Contractor to provide the Service described in the Contract; (ii). Contractor will perform materially as described in the Contract; (iii) the Service is fit for a particular purpose;(iv) Contractor will not interfere with ISC's access to and use of the Service it acquires under the Contract;(v) 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; (vi) 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. If Contractor breaches any of these warranties, ISC may terminate the Contract for cause, without penalty.

10. Data Protection. Protection of personal privacy and ISC Data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized access to or use

of ISC Data, or end-user credit and debit card information, at any time. To this end, the Contractor shall safeguard the confidentiality, integrity, availability, and security of ISC Data and end-user credit and debit card information, including compliance with section 28-51-103, Idaho Code, and comply with the following conditions:

A. All Non-Public ISC Data and end-user credit and debit card information 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 ISC Data and end-user credit and debit card information. 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 level of protection and encryption for all Non-Public ISC Data and end-user credit and debit card information shall be identified in the Contract.

C. At no time shall any ISC Data or processes, that either belong to or are intended for the use of ISC 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 ISC.

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 ISC and its end users solely from data centers within the United States; and storage of ISC Data and end-user credit card information at rest shall be located solely in data centers within the United States. The Contractor shall not allow its personnel or subcontractors to store ISC 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 ISC Data and ISC-written applications and end-user credit and debit card information. If Contractor will be storing, processing, or transmitting ISC data or end-user credit and debit card information through an IaaS or PaaS provider, Contractor must provide a letter from the IaaS/PaaS stating Contractor is a customer in good standing and which environment ISC data or end-user credit and debit card information will be stored, processed, and transmitted. ISC should be notified, in writing, of a data location change within ten (10) calendar days or other timeframe as may be mutually agreed upon by the parties.

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

G. The Contractor shall employ a government-rated cloud compartment to better protect sensitive or regulated ISC data and end-user credit or debit card information.

11. Security Responsibilities. Contractor is responsible for all security. Any shared security responsibilities must be identified with the Proposal and resulting Contract.

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

A. Notify the ISC-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 ISC Data and end-user credit and debit card information from external access, (2) cooperate with ISC as requested by ISC to investigate and resolve the Security Incident or Data Breach, (3) promptly implement remedial measures, if necessary, (4) (for a Data Breach of Non-Public ISC Data only) identify to ISC, if the following is known by the Contractor, the persons affected, their identities, and ISC Data and end-user credit and debit card information 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. For all Data Breaches, the Contractor shall bear the costs associated with the investigation and resolution of the Data Breach and complete all corrective actions as reasonably determined by Contractor based on root cause. For a Data Breach of Non-Public ISC Data or end-user credit and debit card information only, the Contractor shall also bear the costs associated with (1) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to by ISC and the Contractor; (2) a credit monitoring service required by state (or federal) law or as otherwise agreed to by ISC and the Contractor; and (3) 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.

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 ISC and the Contractor in writing, defined by law or contained in the Contract. Discussing Security Incidents with ISC must be handled on an urgent as needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon between ISC and the Contractor in writing, defined by law or as delineated in the Contract.

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

14. Background Checks and Security Awareness. Upon the request of ISC, 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 ISC. If any Contractor Staff are not acceptable to ISC in its sole opinion based upon the results of a criminal background check, ISC, 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 ISC'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 ISC must provide an unredacted version of the audit report to the designated ISC representative no later than thirty (30) calendar days after the report is published. A Service Organization Control (SOC) 2 Type 2 audit report is required, or, ISC may, in its sole discretion, approve another audit type upon Contractor request. In addition, ISC 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. If any audit referenced herein uncovers flaws that potentially materially degrade the protection of the confidentiality, integrity, availability, or security of ISC Data or end-user credit and debit card information, the Contractor shall resolve the flaw or implement a compensating control within a reasonable period of time. Contractor shall notify ISC in writing if Contractor intends to change data centers (e.g. moving from AWS to Azure or between physical hosted data centers), at least ten (10) calendar days prior to such change or as otherwise mutually agreed upon by the parties. If the security standards of the new data center do not meet or exceed the security standards of the previous data center and the standards required in the Contract, the ISC may terminate this Contract without penalty, notwithstanding any other provision to the contrary.

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 ISC of any Updates that may impact availability of Service or performance. Contractor must provide Updates to ISC 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 ISC'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 ISC Data and end-user credit and debit card information 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. ISC shall have the ability to import or export all or portions of ISC 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 ISC to import or export ISC Data and ISC-written applications to and from other entities.

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

C. The return of ISC Data and ISC-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 ISC's extraction of ISC Data and ISC-written applications by providing ISC with all necessary access and tools for extraction, at no additional cost to ISC.

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

E. In the event of termination or expiration of the Contract, the Contractor shall not take any action to intentionally erase ISC Data or ISC-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 ISC Data or to maintain any ISC-written applications and shall thereafter, unless legally prohibited, delete all ISC Data and ISC-written applications (in all forms) within its systems or otherwise in its possession or under its control, unless otherwise instructed by ISC. ISC Data and ISC-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 ISC no later than ninety (90) calendar days after termination or expiration of the Contract.

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

20. Access to Security Logs and Reports. The Contractor shall provide reports to ISC; or alternatively, provide ISC 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 ISC Data.

21. Penetration Tests and Security Assessments. ISC reserves the right to conduct risk assessments, vulnerability assessments, and penetration tests or hire a third party to conduct risk assessments, vulnerability assessments, and penetration tests of the Contractor's application or environment. The Contractor will be alerted in advance and arrangements will be made for an agreeable time. If any penetration test or security assessment referenced herein uncovers flaws that potentially materially degrade the protection of the confidentiality, integrity, availability, or security of ISC Data or end-user credit and debit card information, the Contractor shall resolve the flaw or implement a compensating control within a reasonable period of time.

22. ISC Risk and Authorization Management. ISC has established a National Institute of Standards and Technology (NIST) SP 800-53 revision 4 based process to assess risk associated with storing, processing and/or transmitting ISC Data with external entities, such as Contractor or subcontractors utilized by Contractor. These entities or vendors can include but are not limited to SaaS, PaaS, or IaaS. If

Contractor or a subcontractor utilized by Contractor has been issued a Federal Risk and Authorization Management Program (FedRAMP) Authorization or a StateRAMP Authorization, they will need to submit their FedRAMP or StateRAMP System Security Plan (SSP) to ISC for review. This SSP review is in lieu of the requirement to complete the ISC Baseline Controls spreadsheet. ISC's risk and authorization management process must be completed and reviewed before any relevant work can begin. If a PO has been issued and the Contractor has not completed the required risk review, ISC may terminate the order.

23. ISC Vendor Security Requirements. For RFP and other processes to pre-assess multiple vendors, including Contractor, and for ISC Data requiring Availability only, the ISC Vendor Security Requirements must be completed. The Contractor will be provided with a document to complete and return to ISC for review.

24. Injunctive Relief. Contractor agrees that: (i) no adequate remedy exists at law if it fails to perform or breaches any of the provisions of the Contract regarding confidentiality, availability, integrity, and security of ISC Data and end-user credit and debit card information; (ii) it would be difficult to determine the damages resulting from its breach, and such breach would cause irreparable harm to ISC; and (iii) a grant of injunctive relief provides the best remedy for any such breach, without any requirement that ISC prove actual damage or post a bond or other security. Contractor waives any opposition to such injunctive relief or any right to such proof, bond, or other security. (This section does not limit either party's rights to injunctive relief from breaches not listed.)

25. Compliance of Contractor's Employees and Subcontractors. Contractor must ensure that Contractor's employees and subcontractors comply with, and are subject to a policy or written agreement to comply with, all provisions of the Contract regarding confidentiality, availability, integrity, and security of ISC Data and end-user credit and debit card information (including but not limited to Section 10 of this attachment), that are applicable to the work they perform under the Contract.