**EXHIBIT C: INFORMATION TECHNOLOGY TERMS AND CONDITIONS**

**Contract No. [Contract Number]**

These Terms and Conditions are between the

**State of Montana**

**[Agency Information]**

**(State)**

And **[Contractor Information]**

**(Contractor)**

**THIS EXHIBIT APPLIES TO ALL INFORMATION TECHNOLOGY-RELATED STATE CONTRACTS and MUST BE INCLUDED AS AN ATTACHMENT WITH PRIORITY OVER ALL RFP, PROPOSAL, AND VENDOR DOCUMENTS (*See* Information Technology Definitions, 2-17-506, MCA).**

1. **IT Oversight**
   1. **CIO Approval**

Contractor is notified that, under the provisions of 2-17-514, MCA, the Department of Administration retains the right to cancel or modify any contract, project, or activity that is not in compliance with the Agency’s Plan for Information Technology, the State Strategic Plan for Information Technology, or any statewide IT policy or standard.

* 1. **CIO Oversight**

The Chief Information Officer (CIO) for the State of Montana, or designee, may perform oversight activities. Such activities may include the identification, analysis, resolution, and prevention of deficiencies that may occur while Contractor is performing services. The CIO may require the issuance of a Right to Assurance or may issue a Stop Work Order.

* 1. **Right to Assurance**

If State, in good faith, has reason to believe that Contractor does not intend to, is unable to, or has refused to perform or continue performing all material obligations under these Terms and Conditions, State may demand in writing that within a certain number of days (no less than 5 business days) specified in the demand for Contractor to provide a written assurance of intent to perform. State may, at State’s option, find this a basis for termination allowing State to pursue all available rights and remedies.

* 1. **Stop Work Order**

State may, at any time by written order to Contractor require Contractor to stop any or all parts of required work for the period of days indicated by State after the order is delivered to Contractor. This order must be specifically identified as a Stop Work Order (SWO) issued under these terms and conditions. Upon receipt of the SWO, Contractor shall immediately comply with its terms and take all reasonable steps to minimize incurrence of costs allocable to the work covered by the SWO during the period of work stoppage. If a SWO issued under these terms and conditions is canceled or the period of the order or any extension expires, Contractor shall resume work. State’s Contract Manager shall make the necessary adjustment in the delivery schedule or price, or both, and the services shall accordingly be amended in writing.

* 1. **Remote Access**

Contractor agrees that Montana information technology resources will not be accessed by Contractor, including all officers, employees, agents, subcontractors, affiliated users, and any subcontractors located outside of the legal jurisdictional boundary of the United States (outside of the United States, its territories, embassies, or military installations).

1. **Blind or Visually Impaired Access**

No State funds may be expended for the purchase of information technology equipment and software for use by employees, program participants, or members of the public unless it provides blind or visually impaired individuals with access, including interactive use of the equipment and services, that is equivalent to that provided to individuals who are not blind or visually impaired. (18-5-603, MCA.) State Procurement Services Division at (406) 444-2575 has more information concerning nonvisual access standards.

1. **IT Accessibility Requirements**

Contractor understands and agrees to comply with federal law on or before April 24, 2026, if applicable, in compliance with Health and Human Services (HHS) Section 508 and Accessibility Standards Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220), which requires that when State develops, procures, maintains, or uses information and communication technology (ICT), it shall be accessible to people with disabilities. State employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities. All products, platforms and services delivered as part of this Contract that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 CFR 1194.1 & Apps. A, B, & C, and available at https://www.access-board.gov/ict/. All requirements are applicable to support services and deliverables. All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT. For each proposed product or platform, a fully completed Accessibility Conformance Report (ACR) using the Voluntary Product Accessibility Template (VPAT) must be submitted. See (https://www.itic.org/policy/accessibility/vpat) or HHS conformance checklist(s) (https://www.hhs.gov/web/section-508/accessibility-checklists/index.html). Prior to commencing performance, Contractor must demonstrate conformance to the HHS Section 508 requirements via HHS Section 508 checklist(s) (https://www.hhs.gov/web/section508/accessibility-checklists/index.html). State reserves the right to perform testing on required ICT items to validate Contractor’s Section 508 conformance claims. If State determines at any time that Section 508 conformance does not meet the HHS Section 508 requirements, State shall, at its option, require Contractor to remediate the item, at no additional fee or cost to State and align with HHS Section 508 conformance requirements or immediately terminate this Contract with no additional fee or cost to State.

1. **Subcontractor**

Contractor shall be responsible for ensuring its subcontractors comply with these terms and conditions.

1. **Security Awareness**

Upon request, Contractor agrees to certify that Contractor’s officers, employees, agents, subcontractors, and affiliated users with access to State information technology data, digital access systems, information technology resources, or telecommunications networks (2-17-506, MCA) have completed security awareness training within the past 12 months before gaining access to State information technology resources or may complete State-approved annual security awareness training.

1. **State-Approved Criminal Background Checks**

Contractor warrants to only assign employees and subcontractors who have annually completed and passed a background check. With Contractor’s access to particularly sensitive data and at State’s request, Contractor’s employees and subcontractors shall complete an additional State IT background check.

1. **Physical Activities and Spoofing**
   1. **Physical Activities**

Contractor and its officers, employees, agents, affiliated users, and any subcontractors shall not violate or attempt to violate the security of State’s network or interfere or attempt to interfere with State’s systems, networks, authentication measures, servers or equipment, or with the use of or access to State’s network by any other user.

* 1. **Spoofing**

Contractor agrees to use State’s secure email relay for sending email from cloud services to its users. Additionally, Contractor shall not perform unauthorized spoofing or scanning of any kind, including user account identity. Contractor’s systems shall not spoof the mt.gov domain or engage in email spoofing. Email spoofing is the creation of email messages with a forged sender address to create or send emails using State’s domain. Such prohibited activity includes but is not limited to:

1. Accessing or logging into a State server where access is not authorized;
2. Unauthorized probing, scanning, or testing the security or vulnerability of State’s network or other systems; and/or
3. Attempting to portray itself as State or an affiliate of State or otherwise attempting to gain access, without authorization, via State’s network or systems to any State account or information technology resource not belonging to Contractor or its officers, employees, agents, subcontractors, and affiliated users.
4. **Linked Terms and Conditions**

The parties specifically agree that any language or provisions contained on either party’s website or product schedule, or contained in any “shrinkwrap” or “clickwrap” agreement shall be of no force and effect and shall not in any way supersede, modify or amend these Terms and Conditions.

1. **Cyber Security Insurance**

Contractor shall purchase and maintain cyber/information security insurance coverage with combined single limits for each wrongful act of $6,000,000 in the aggregate to cover unauthorized acquisitions of personal information such as social security numbers, credit card numbers, financial account information, or other information that uniquely identifies an individual and may be of a sensitive nature in accordance with 2-6-1501-1503, MCA. If Contractor maintains higher limits than the minimums shown above, State requires and shall be entitled to coverage for the higher limits maintained by Contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to State. Such insurance must cover, at a minimum, privacy notification costs, credit monitoring, forensics investigations, legal fees/costs, regulatory fines and penalties, and third-party liability settlements or judgments as may be caused by any act, omission, or negligence of Contractor’s officers, agents, representatives, assigns or subcontractors. Note: if occurrence coverage is unavailable or cost-prohibited, State will accept “claims made” coverage provided the following conditions are met: 1) the retroactive date must be shown, and must be before the date of the Contract or the beginning of the Contract work; 2) insurance must be maintained and evidence of insurance must be provided for at least three (3) years after completion of the Contract of work; and 3) if coverage is cancelled or non-renewed and not replaced with another claims-made policy form with a retroactive date prior to the Contract effective date, Contractor must purchase “extended reporting” coverage for a minimum of three (3) years after completion of work.

1. **Intellectual Property Rights**

In the event State suggests or requests any modifications or improvements to Contractor’s software which are implemented by Contractor, such modifications or improvements shall become the sole property of Contractor. All right, title and interest in software, and all copyrights, patents, trademarks, service marks or other intellectual property or proprietary rights relating thereto, belong exclusively to Contractor.

1. **Title and Ownership Rights**

State retains title to and all ownership rights in all State data and content provided by State ("Content"), including but not limited to multimedia or images (graphics, audio, and video), text, and the like, and grants Contractor the right to access and use Content for the purpose of complying with its obligations under this Contract and any applicable Statement of Work.

1. **Violation of Terms and Conditions Sanction**

Violation of these terms and conditions may also be a violation of state and federal law and include both civil and criminal penalties.

1. **Indemnification**

State shall not indemnify Contractor or its subcontractor.

1. **Information Technology Resource Categories**

The services provided by Contractor involve the following information technology resources (check all that apply):

|  |  |
| --- | --- |
| On premise system services | On premise system  Software  Hardware |
| Internet Of Things Systems | Professional IT Services |
| SaaS | Cloud System |
| PaaS | Not listed [please describe] |
| IaaS |  |

1. **Data and Security**

**NOTE:** (Check the box of the highest classification of public and non-public data owned by State that may be stored, transmitted, accessed, or processed by the IT resources provided under this Contract or related to the services provided by Contractor under this Contract.) A checkmark () in the corresponding column indicates the IT Terms and Conditions shown in the table below apply to this Contract.

**No Data** (such as IT peripherals)

**Public Data - mapped to Federal Information Processing Standards (FIPS) 199 LOW.** “Low Level Data” is information residing in information systems categorized as Low and available to the general public and eligible for public access.

**Non-public Data - mapped to FIPS 199 MODERATE.** “Moderate Level Data” is information residing in information systems categorized as Moderate and governed by specific laws on disclosure to third parties or the public which determine and protect confidentiality.

**Non-public Data - mapped to FIPS 199 HIGH**. “High Level Data” is information residing in information systems categorized as High and, if divulged, could compromise or endanger citizens, employees, or safety assets of State. (A separate Data Level Contract will be attached.)

|  |  |  |  |
| --- | --- | --- | --- |
| **Public Data (Low)** | **Non-Public Data (Moderate)** | **Section Heading** | **IT Terms and Conditions** |
| Checkmark with solid fill | Checkmark with solid fill | **Data Ownership and Access** | **Data Ownership**  State owns all right, title, and interest in its data that is related to the services provided. State data may also include data from a third party.  **Data Access**  Contractor shall not access State of Montana user accounts, or State data, except: (i) in response to service or technical issues; (ii) as required by the express terms of services engagement document; or (iii) at State’s written request. |
|  | Checkmark with solid fill | **Data Location** | **Data Location**  Contractor shall not store, process, or transfer any non-public State data outside of the United States, including for services or back-up and disaster recovery purposes. |
| Checkmark with solid fill | Checkmark with solid fill | **Data Disclosure and Usage** | **Data Disclosure-Prohibition**  At no time will any information belonging to or intended for State, be copied, disclosed, or retained by Contractor or any party related to Contractor for subsequent use in any transaction.  **Confidential Data-Usage**  Contractor will take reasonable steps to limit the use of, or disclosure of, and requests for, confidential State data to the minimum degree necessary to accomplish the services. Privacy protection of personal identifiable information, personal identifiable health information, and sensitive data shall be an integral part of the business activities of Contractor to ensure that there is no inappropriate or unauthorized use of State information at any time.  **Limitation on Usage to Purpose of Services**  Contractor shall not use any information collected for any purpose other than fulfilling the service.  **Data Safeguards**  Contractor shall safeguard the confidentiality, integrity, and availability of State information.  **Subsequent Use**  Contractor shall not use any data for subsequent use that has not been expressly authorized in writing by State.  **Syndicated Data**  Contractor shall not use State data to create syndicated data unless expressly authorized by State in writing. |
| Checkmark with solid fill | Checkmark with solid fill | **Authorized Personnel** | **Authorized Personnel**  Only duly authorized personnel will have access to State data and may be required to obtain security clearance from State prior to accessing State data. |
| Checkmark with solid fill | Checkmark with solid fill | **Use of AI** | **Use of AI or State Sub Domain:** Prior to performance, Contractor must inform State of any generative Artificial Intelligence (“AI”) in Goods or Services relating to this Contract. Additionally, utilization of generative AI in the creation of Goods and Services impacting State’s Intellectual Property Rights shall include annotations citing source materials.  Contractor is prohibited from using State materials or data in generative AI queries or from building training proprietary generative AI programs without prior written permission from State. Contractor attests that its AI models use only properly licensed material. Should Contractor be found in violation of this requirement, Contractor shall fully indemnify and defend State from all claims related thereto. Should Contractor learn that State materials or data has been used in generative AI queries without permission from State, Contractor shall immediately notify State of the use and cover the full expense of any remediation. |
|  | Checkmark with solid fill | **Breach and Notification** | **Notification to State**  Without unreasonable delay, Contractor must notify the State of Montana Chief Information Security Officer of any incident resulting in the destruction, loss, unauthorized disclosure, or alteration of State of Montana data.  **Notification to Person**  Upon discovery or notification of a breach of the security of a data system, Contractor shall comply with 2-6-1503, MCA, which includes unencrypted data. Without unreasonable delay, consistent with the legitimate needs of law enforcement, Contractor shall make reasonable efforts upon discovery or notification to the impacted State agency of a breach and will notify any person whose personal information is **r**easonably believed to have been acquired by an unauthorized person. This notification may be delayed at the request of law enforcement.  **No Limitation of Liability Contractor IT Negligence**  Contractor cannot limit its liability to relieve Contractor or its subcontractors from its own security incident or data breach that materially compromises the security, confidentiality, or integrity of personal information maintained by a state agency or by a third party on behalf of a state agency (2-6-1501, MCA), negligence, or to the extent that it creates an obligation on the part of State to indemnify or hold a Contractor harmless. |
| Checkmark with solid fill | Checkmark with solid fill | **Termination and Suspension of Service** | **Suspension of Services**  During any period of suspension, negotiation, or disputes, Contractor shall not take any action to intentionally alter, erase, or otherwise render inaccessible any State data.  **Termination of a portion or of the entire services provided.**  In the event of termination of any services or Contract in entirety, Contractor shall not take any action in intentionally alter, erase, or otherwise render inaccessible any State data for a period of 90 days after the effective date of the termination. Within this 90-day timeframe, Contractor will continue to secure and backup State data covered under the provided services. After such 90-day period, Contractor shall have no obligation to maintain or provide any State data. Thereafter, unless legally prohibited, Contractor shall dispose securely of all State data in its systems or otherwise in its possession or control, as specified herein.  **Post-Termination Assistance**  State shall be entitled to any post-termination assistance generally made available with respect to the Services unless unique data retrieval arrangements has been established as part of the Contract or Service Level Agreement. |
|  | Checkmark with solid fill | **Data Disposition** | State data may be disposed at the termination of services using one of the following methods:   1. **State Removal with Contractor’s Tools**   State may remove or destroy State data using Contractor’s tools.   1. **Contractor to Return State Data**   Contractor will account for and return all State data in all of its forms. The data shall be returned in a format acceptable to State. At no time shall any data or processes that either belong to or are intended for the use of State or its officers, agents, or employees, be copied, disclosed, or retained by Contractor.   1. **Contractor to Destroy State Data**   When required by State, Contractor shall destroy all requested data in all forms. Data shall be permanently deleted, and shall not be recoverable, in accordance with National Institute of Standards and Technology (NIST) SP 800-88 “Media Sanitization Guidelines.”   1. **Certificate of Destruction**   In all cases, Contractor will certify that all State information process during the performance of the services will be completely purged from all physical and electronic data storage with no output to be retained by Contractor at the time the work is completed, the Contract is terminated, or upon written request of State. |
| Checkmark with solid fill | Checkmark with solid fill | **Notification of Legal Requests** | **Notification of Requirement to Access State Data**  Contractor shall contact State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to State data.  **Legal Request for State Data**  Regarding State data and processes, Contractor shall not respond to subpoenas, service of process, and other legal requests without first notifying State unless prohibited by law from providing such notice. |
| Checkmark with solid fill | Checkmark with solid fill | **Data Encryption** | **In Transit and At Rest**  Contractor shall encrypt all data in transit, regardless of transit mechanism, and at rest.  **Encryption Standards**  Contractor’s encryption shall meet validation cryptography standards as specified by NIST in FIPS 140-2 (or latest revision) and subsequent security requirements or guidelines. Contractor and State will negotiate mutually acceptable key location and key management details. |
| Checkmark with solid fill | Checkmark with solid fill | **System Security** | **Contractor Responsibility**  Contractor shall ensure systems delivered are adequately secure. Adequate security is defined to require compliance with Federal and State of Montana security requirements and to ensure freedom from those conditions that may impair State’s use of or permit unauthorized access to State’s data or IT.  **State Security Policy, Framework, Standards and Controls**  State has established security policy, framework, standards, and controls that align with the NIST Cybersecurity Framework. The latest revision of NIST (SP 800-53) is used for control adherence evaluation established after developing a security categorization utilizing FIPS PUB 199 (or latest revision).  **Managerial, Operational, and Technical Controls**  All computer systems receiving, processing, storing, or transmitting State data must meet the control requirements for the associated security categorization within NIST SP 800-53 (or latest revision). To meet functional and assurance requirements, the security features of the environment must provide managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to State data.  **Independent Security Audits**  Contractor shall provide reasonable proof, through independent audit reports, typically AICPA SOC 2 Type 2 (or latest version), that the system specified in delivering the services meets or exceeds federal and State security requirements to ensure adequate security and privacy, confidentiality, integrity, and availability of State’s data and information technology.  **Annual Assurance**  The delivery of annual assurance statements shall be facilitated by the Contract Manager. Annual assurance statements must contain a detailed accounting of the security controls implemented.  **Security Audits and Annual Statements**  State considers the security audits and annual statements to be confidential and upon Contractor’s request, will route a Nondisclosure Agreement. In compliance with SOC 2 security compliance, State will destroy all confidential information upon completion of any Security Audit or review of Annual Statements.  **System Security Plan**  Contractor agrees to include within their Statement of Work a provision assisting with the creation of a System Security Plan (SSP). State may require Contractor to supply a Cloud/Customer Responsibility Matrix which denotes responsibilities as either Shared Contractor or State. |
| Checkmark with solid fill | Checkmark with solid fill | **Security Standard Compliance Certificate** | **Security Certification**  Contractor shall meet, and provide proof of, one or more of the following Security Certifications.   * GovRAMP- Authorized Product Certification * FedRAMP- Federal Risk and Authorization Management Program * ISO 27001:2013 * HITRUST CSF * Other industry-recognized certification, as approved by State and only if Contractor cannot provide one of the above certifications. |

|  |  |
| --- | --- |
| **Chief Information Officer Approval:** |  |
| Contractor is notified that, under the provisions of 2-17-514, MCA, the Department of Administration retains the right to cancel or modify any contract, project, or activity that is not in compliance with the Agency's Plan for Information Technology, the State Strategic Plan for Information Technology, or any statewide IT policy or standard. | |
| Approved ITPR #: [Enter Approved ITPR #] |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Chief Information Officer | Date |
| Department of Administration |  |

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Vendor Authorized Signature | Date |