**ATTACHMENT B: STATE OF UTAH STANDARD INFORMATION TECHNOLOGY TERMS AND CONDITIONS**

This is for a contract of information technology products and services and must be accompanied by the State of Utah Standard Terms and Conditions for Goods and Services as Attachment A. In addition to the definitions in this Attachment B, the definitions in Attachment A apply to this attachment. If a term is defined in both Attachment A and Attachment B, the definition in Attachment B will govern. All policies referenced by number in this Attachment B are available at<https://dts.utah.gov/policies>. Other policies are available upon request.

1. **DEFINITIONS:**
	1. “Access to Secure State Facilities, Data, or Technology” means Contractor will (a) enter upon secure premises controlled, held, leased, or occupied by State of Utah; (b) maintain, develop, or have access to any deployed hardware, software, firmware, or other technology that is in use by State of Utah; or (c) have access to or receive State Data or State confidential information, or both.
	2. “Authorized Persons” means the Contractor’s employees, officers, partners, Subcontractors, or agents of Contractor who need Access to Secure State Facilities, Data, or Technology to enable the Contractor to perform its responsibilities under this Contract.
	3. “Contract Period” means the term of this Contract, as set forth in the Contract Signature Page(s).
	4. “Custom Deliverables” means the product that Contractor is required to design, develop, or customize and deliver to a State Entity as specifically described under this Contract or an associated statement of work for which all interest and title shall be transferred to and owned by the State Entity. This includes every invention, design, development, customization, improvement, process, software program, work of authorship, documentation, formula, datum, technique, know how, or intellectual property right whatsoever or any interest therein (whether patentable or not patentable or registrable under copyright or similar statutes or subject to analogous protection) that is specifically made, conceived, discovered, or reduced to practice by Contractor pursuant to this Contract.
	5. “Data Breach” means the unauthorized access to or acquisition, disclosure, loss of access, or destruction of State Data that compromises the security, confidentiality, or integrity of State Data.
	6. “DGO” means the Utah Department of Government Operations.
	7. “DTS” means the Utah Department of Government Operations Division of Technology Services.
	8. “Federal Criminal Background Check” means a fingerprint-based, nationwide background check conducted and processed by the FBI.
	9. “Federal Data” means all information that originated with a federal entity, including federal tax information.
	10. “Good” means any deliverable not classified as a Custom Deliverable or Service.
	11. “Intellectual Property Rights” means all rights to patents, utility models, mask works, copyrights, trademarks, trade secrets, and other protection afforded by law to inventions, models, designs, technical information, and applications.
	12. “Non-Public Data” means records or data that are not subject to distribution to the public. Access is restricted because it includes information that is protected by state or federal law. Non-Public Data includes, but is not limited to, a person’s name; government-issued identification numbers (e.g., Social Security, driver’s license, passport); financial account information; or Protected Health Information.
	13. “Personal Data” means information, whether by itself or combined with other data elements, that can identify an individual with reasonable specificity or that is linked or can be reasonably linked to an identified individual.
	14. “Procurement Item” means a Good, a supply, a Service, Custom Deliverable, construction, or technology that Contractor is required to deliver to the State of Utah under this Contract, including software and Software as a Service.
	15. “Protected Health Information” (PHI) is as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and its implementing regulations.
	16. “Security Incident” means the attempted unauthorized access to State Data or Personal Data that may result in the use, disclosure, or theft of State Data or Personal Data. Consistent with the GDPA at Subsection 63A-19-405(1)(b), a governmental entity must report “the unauthorized access, acquisition, disclosure, loss of access, or destruction of data that compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the governmental entity”. An incident does not include unsuccessful pings and port scans.
	17. “Service(s)” means the furnishing of labor, time, or effort by Contractor, and may include installation, configuration, implementation, technical support, warranty maintenance, and other support services.
	18. “Single Sign On” means the authentication and authorization system operated by the State of Utah for accessing resources operated either by the State or a third party on behalf of the State.
	19. “State Data” means all Confidential Information, Non-Public Data, and Personal Data that is created, controlled, maintained, owned, or in any way originating from or on behalf of the State of Utah, and all State-controlled data that is the output of computer processing or other electronic manipulation of any data the State created, controlled, maintained, or in any way originated from the State of Utah, regardless of where such data or output is stored or maintained.
	20. “StateRAMP dba GovRAMP” means a Risk and Authorization Management Program, which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by state and local governments, public education institutions, and special districts enabling these organizations to validate the security of their third-party IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and/or SaaS (Software as a Service) solutions which process, transmit, and/or store the organization’s data or which could impact data security. GovRAMP’s security verification model is based on NIST 800-53 Rev. 5 published by the National Institute of Standards and Technology (NIST). Moving forward GovRAMP will be the name used.
	21. “GovRAMP Progressing Snapshot” means a program within the GovRAMP framework that utilizes a predetermined set of NIST 800-53 controls for quarterly evaluations and monthly advisory calls. This program aims to identify and address deficiencies in the security of cloud products, ensuring continuous improvement and compliance with GovRAMP standards.
	22. “GovRAMP Verified Status” means a status indicating that a service provider has met all GovRAMP security requirements related to that status and has been provided with an authorization established by the GovRAMP governing boards including but not limited to Ready, Core, Authorized or Provisionally Authorized.
	23. “Subcontractors” means contractors, manufacturers, distributors, suppliers, or consultants, at any tier, that are under the direct or indirect control or responsibility of Contractor, including a person or entity that is, or will be, providing goods or performing services pursuant to this Contract.
	24. “X [Software, Platform, Infrastructure, Network, etc.] as a Service” means an application running on a Contractor’s or the State of Utah’s cloud infrastructure, which is 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 State 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

**General Provisions**

1. **SOVEREIGN IMMUNITY:** The State of Utah does not waive any protection, right, defense or immunity under the Governmental Immunity Act of Utah, Utah Code §§ 63G-7-101 to 904, as amended, the Eleventh Amendment to the Constitution of the United States, or otherwise, from any claim or from the jurisdiction of any court. If a claim must be brought in a federal forum, then it must be brought and adjudicated exclusively within the United States District Court for the District of Utah. This paragraph only applies to a claim brought against the State of Utah to the extent Congress has abrogated the State of Utah’s sovereign immunity and this paragraph is not consent by the State of Utah to be sued in federal court.
2. **DRUG-FREE WORKPLACE:** Contractor shall abide by DTS’s drug-free workplace policy 2000-0017 when it is accessing Non-Public Data, or while it is on the State of Utah’s premises.
3. **CODE OF CONDUCT:** If Contractor is working at facilities controlled or owned by DTS or the State of Utah, Contractor shall follow and enforce the DGO Code of Conduct, DTS Policy 1000-0003 Acceptable Use of Information Technology Resources and the agency applicable code of conduct. Contractor will ensure that each employee working at such facilities receives a copy of the policies and applicable codes of conduct.
4. **WEBSITE BRANDING:** Contractor shall only use the approved executive branch agency and/or State of Utah logo on websites produced under terms of this Contract. This provision is separate from and in addition to the publicity clause in the state’s general terms and conditions, such as those contained in Attachment A.
5. **CONTRACTOR’S INSURANCE RESPONSIBILITY:**
	1. If Contractor has access to State Data, Contractor shall maintain Cyber Security Coverage from an insurance company authorized to do business in the State of Utah. The insurance policy must cover data breach and privacy/cyber liability including technology errors and omissions and professional liability. For low risk data, the limits will be no less than $2,000,000.00 aggregate. For moderate risk data, the limits will be no less than $5,000,000.00 aggregate. For high risk data, the limits will be no less than $10,000,000.00 aggregate. Data risk categories are as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.
	2. Before this Contract commences, Contractor shall deliver to the State Entity a Certificate of Insurance showing up-to-date coverage. Failure to provide a Certificate of Insurance throughout the Contract Period will constitute a material breach of the Contract. Further, the State Entity reserves the right to withhold any payments to Contractor until a Certificate of Insurance has been delivered, and withholding payment will not be considered a remedy for the breach, nor will it affect or limit the State Entity’s available remedies set forth under this Contract.
	3. Contractor’s failure to maintain this insurance requirement for the Contract Period will be grounds for immediate termination.
6. **RIGHT TO MONITOR PERFORMANCE AND AUDIT**
	1. **Audit:** Contractor shall, upon written notification, permit the State of Utah, or a third party designated by the State of Utah, to perform an assessment, audit, examination, or review of all of Contractor’s sites and environments related to the State of Utah’s records or State Data - including physical, technical, and virtual sites and environments - in order to confirm Contractor’s compliance with this Contract, associated scopes of work, and applicable laws, regulations, and industry standards. Contractor shall fully cooperate with such assessment by providing access to knowledgeable personnel; physical premises; records; technical and physical infrastructures; and any other person, place, or object which may assist the State of Utah or its designee in completing such assessment. Upon request, Contractor shall provide the results of any audit performed by or on behalf of Contractor that would assist the State of Utah or its designee in confirming Contractor’s compliance with this Contract; associated scopes of work; and applicable laws, regulations, and industry standards. If Federal Data is involved, this provision may not be waived to restrict Federal audit requirements.
	2. **Monitor Performance**: The State Entity reserves the right to monitor Contractor’s performance, perform plan checks, plan reviews, other reviews, and/or comment upon the Services of Contractor. This includes Contractor’s Subcontractors, if any. Results of any evaluation may be made available to the Contractor upon Contractor’s request.
	3. **GovRAMP Continuous Monitoring**: The Contractor is required to grant access to GovRAMP Continuous Monitoring and reporting for a product utilizing a GovRAMP Security Progressing Snapshot, Core, Ready, Provisionally Authorized or Authorized status throughout the life of the Contract. DTSreserves the right to request and review all Third-Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of the Contractor’s environment. The Contractor shall respond to all flaws discovered by providing a mutually agreed upon timeframe to resolve the issue and/or implement a compensating control.
	4. **Contract Compliance:** If Contractor's performance involves the payment card industry, Contractor will obtain a third-party PCI compliance report annually and submit the same to the State upon request. In no event shall the PCI compliance report be more than 12 months old at the time it is provided to the State.
7. **SURVIVORSHIP:** The contractual provisions that will remain in effect after expiration or termination of this Contract are: (a) Secure Protection and Handling of State Data; (b) Data Breach Responsibilities; (c) ownership in Custom Deliverables; (d) ownership, protection, and use of records, including residuals of such records; and (e) Ownership, Protection, and Use of Confidential Federal, Utah, or Local Government Internal Business Processes, including residuals of such confidential business processes; (f) Ownership, Protection, and Return of Documents and Data Upon Contract Termination or Completion; (g) conflict of terms; and (h) any other terms that by their nature would survive the expiration, completion, or termination of this Contract.
8. **TERMINATION FOR CONVENIENCE:** Any Procurement Item may be terminated in whole or in part without cause (for convenience), in advance of the specified renewal date, by the State Entity, upon thirty (30) days written termination notice being given to the Contractor. The State Entity will not be liable for any costs or fees that would have been incurred following the notified date of termination, notwithstanding any other provision in the Contract, purchase order, or vendor quote.
9. **COMPLIANCE WITH ACCESSIBILITY STANDARDS:** Contractor shall comply with Utah Administrative Code R895-14-3(3), which states that contractors developing websites, hardware, or software for State agencies are required to comply with applicable accessibility guidelines.
10. **TIME IS OF THE ESSENCE:** The Services shall be completed and Goods and Custom Deliverables delivered by any applicable deadline stated in this Contract. Time is of the essence.
11. **STANDARD OF CARE:** For Services of Contractor which require licenses and certifications, such Services shall be performed in accordance with the standard of care exercised by licensed members of their respective professions having substantial experience providing similar services which similarities include the type, magnitude, and complexity of the Services that are the subject of this Contract.
12. **HARDWARE WARRANTY:** **THE STATE OF UTAH DOES NOT ACCEPT ANY PROCUREMENT ITEM “AS-IS”.** Contractor warrants all hardware portions of any Good or Custom Deliverable that it directly or indirectly provides for a period of **one year**. All warranties granted to the State Entity by the uniform commercial code of the State of Utah apply to this Contract. Product liability disclaimers and/or warranty disclaimers from Contractor or its suppliers are rejected. Contractor warrants that the hardware: (a) will perform as specified in the response; (b) will live up to all specific claims listed in the response; (c) will be suitable for the ordinary purposes for which the hardware is used; (d) will be suitable for any special purposes that the State Entity has relied on Contractor’s skill or judgment to consider when it advised the State of Utah about the hardware in the response; (e) the hardware has been properly designed and manufactured; and (f) is free of significant defects.
13. **SOFTWARE WARRANTY: THE STATE OF UTAH DOES NOT ACCEPT ANY PROCUREMENT ITEM “AS-IS”.** Contractor warrants for a period of **one year** from the date of acceptance that the software portions of the Goods and Custom Deliverable, including Software as a Service, that Contractor directly or indirectly provides will: (a) perform in accordance with the specific claims provided in the Response and all specifications and documentation for the software; (b) be suitable for the ordinary purposes for which such goods and custom deliverables are used; (c) be suitable for any special purposes that the State of Utah has relied on Contractor’s skill or judgment to consider when it advised the State about the Goods or Custom Deliverables; (d) have been properly designed and manufactured; and (e) be free of significant defects. Contractor shall provide the State of Utah with bug fixes and inform the State Entity of any known software bugs or software defects that may affect the State Entity’s use of the software. Product liability disclaimers and/or warranty disclaimers from Contractor or its suppliers are rejected
14. **WARRANTY REMEDIES:** Upon breach of the hardware or software warranty, Contractor will promptly repair or replace (at no charge to the State of Utah) the nonconforming Goods or Custom Deliverables. If the repaired and/or replaced products are inadequate, Contractor will refund the full amount of any payments that have been made during the warranty period for the failed products. These remedies are in addition to any other remedies provided by law or equity.
15. **DEVELOPMENT, TEST, AND PRODUCTION ENVIRONMENTS:** If Goods or Services under this Contract are Contractor-hosted, the Contractor will include three environments throughout the term of the Contract: a development, test, and production environment. Regular refreshes to the database or application or both will be requested. To perform an application refresh (defined as “any promotion of code, regardless of the environment”), all developers involved in the project, whether from the Contractor or the State, will need to approve in writing the refresh request to prevent any code from being deleted without a prior backup. The cost to configure and maintain these environments is included in the Contract price and will not be charged beyond the amount noted on the Contract Cover Page.
	1. If a development or test region is promoted to production, that region must have all of the required security and privacy controls and audit requirements prior to promotion.
	2. If the application cannot perform a production refresh after the application is live, then a secondary environment for testing must be created by Contractor.
	3. If the Contractor chooses not to provide the three separate environments required by the first paragraph of this section 16, the Contractor must configure the production environment with dummy or test accounts that have the ability to go through the full application process without causing or creating data or cost discrepancies. Additionally, a device or mechanism, such as a feature flag/banner announcement to call out new features to the user, or canary releases to allow for gradual release to smaller sets of users, must be included. Logging must be enabled in order to identify and diagnose issues and to fulfill audit and regulatory requirements, including security frameworks such as NIST and OWASP. A/B testing, automated testing, and incremental rollouts must also be considered and clarified in lettered additions to this Section 15 (e.g. “d,” “e,” etc.). A way of communicating upcoming changes via notification, alerts, emails, and updates must be available. Contractor will make clearly defined fallback strategies and rollback plans available prior to any code promotion.

**License and Ownership**

1. **GENERAL LICENSE:** For any software, including SaaS, delivered that is not considered a Custom Deliverable, Contractor grants the State Entity a non-exclusive, non-transferable, right to use, without the right to sublicense, such software for the State of Utah’s internal business operation under this Contract. If the software is perpetual, Contractor grants the State Entity a non-exclusive, non-transferable, irrevocable, perpetual right to use and copy, without the right to sublicense, for DTS’s and the State of Utah’s internal business operation under this Contract.
2. **OWNERSHIP AND USE OF RECORDS:** DTS and the State of Utah shall own exclusive title to all information and data gathered, reports developed, and conclusions reached by the State Entity in performance of this Contract. Contractor may not use, except as specified in the SOW, information gathered, reports developed, or conclusions reached by the State Entity in performance of this Contract without the express written consent of the State Entity. This includes information in anonymized or aggregated formats.
3. **OWNERSHIP AND USE OF DATA:** The State of Utah shall own and retain unlimited rights to use, disclose, or duplicate all information and data (copyrighted or otherwise) specifically developed, derived, documented, stored, or furnished by Contractor for the State Entity under this Contract. Contractor, and any Subcontractors under its control, expressly agrees not to use Non-Public Data without prior written permission from the State Entity and appropriate officials of the State of Utah.
4. **OWNERSHIP, PROTECTION, AND USE OF CONFIDENTIAL FEDERAL, UTAH, OR LOCAL GOVERNMENT INTERNAL BUSINESS PROCESSES AND PROCEDURES:** In the event that the State Entity provides Contractor with confidential federal or state business processes, policies, procedures, or practices, pursuant to this Contract, Contractor shall hold such information in confidence, in accordance with applicable laws and industry standards of confidentiality, and not copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of, give, or disclose such information to third parties or use such information for any purpose whatsoever other than the performance of this Contract. The improper use or disclosure by any party of protected internal federal or state business processes, policies, procedures, or practices is prohibited. Confidential federal or state business processes, policies, procedures, or practices shall not be divulged by Contractor or its Subcontractors, except for the performance of this Contract, unless prior written consent has been obtained in advance from the State Entity.
5. **OWNERSHIP, PROTECTION, AND RETURN OF DOCUMENTS AND DATA UPON CONTRACT TERMINATION OR COMPLETION:** All documents and data pertaining to work required by this Contract will be the property of the State Entity and the State of Utah, and must be delivered to the State Entity upon its request at any time during the Contract Period, as well as within thirty (30) working days after termination or expiration of this Contract, and without restriction or limitation to their future use. Any State Data returned under this section must either be in the format as originally provided, in a format that is readily usable by the State Entity, or formatted in a way that it can be used. Contractor will pay the costs for returning documents and data to the State Entity except as specified in this Contract.

**Technical Support**

1. **UPDATES AND UPGRADES:** Any upgrades and updates provided by Contractor are subject to the terms of this Contract. If Software is on premises, the State Entity reserves the right to accept updates and upgrades at its discretion and to determine if such updates comply with the Security requirements in the Contract. Contractor shall keep any applicable hardware, software, middleware, and application plugins up to date and in a state of good repair. All patches, critical vulnerabilities, and/or hardware issues must be addressed based on response times by criticality as laid out in the SOW. If the State hosts the solution, then Contractor may request such maintenance from the DTS hosting team.
2. **BUG FIXING AND REMOTE DIAGNOSTICS:** Contractor shall use commercially reasonable efforts to provide work-around solutions or patches to reported software problems. If software is on premises, Contractor may perform remote diagnostics to work on reported problems with DTS’s prior written authorization. If DTS declines remote diagnostics, Contractor and DTS may agree to on-site technical support, subject to the terms of the Contract.
3. **TECHNICAL SUPPORT AND MAINTENANCE:** If technical support and maintenance is required by the Contract, Contractor will use commercially reasonable efforts to respond to the State Entity in a reasonable time, and in all events, in accordance with the specific timeframes detailed in the Contract, when the State Entity makes technical support or maintenance requests.
4. **ELECTRONIC DELIVERY:** Contractor may electronically deliver any Good or Custom Deliverable to the State Entity or provide any Good and/or Custom Deliverable for download from the Internet. Contractor shall ensure the confidentiality of electronic deliveries in transit. Contractor warrants that all electronic deliveries will be sent with all reasonable security measures in place to ensure deliverable is free of known malware, bugs, Trojan horses, etc.
5. **TRANSITION ASSISTANCE**: Upon termination or expiration of the Contract, Contractor shall reasonably cooperate with other parties in connection with all Goods and Services to be delivered, including any successor contractor to whom data is transferred. The Contractor shall assist the State Entity in exporting and extracting data, in a format usable without the use of the Procurement Item and as agreed to between the parties, at no additional cost. Any transition service requested by the State Entity involving knowledge transfer and support beyond that described in this paragraph prior to this sentence may be subject to a statement of work at Contractor’s then current rates, agreed upon between the Parties and added by amendment to this Contract.

**Security**

1. **CRIMINAL BACKGROUND SCREENING/DRUG TESTING AND SECURITY TRAINING:** Each employee of Contractor and Subcontractor who will be granted unescorted Access to Secure State Facilities or State Data, or any Access to Technology must successfully complete a Federal Criminal Background Check, in accordance with DTS Policy 2000-0014 Background Investigations, prior to being granted such Access. Contractor or the applicable employee shall provide DTS with sufficient personal information (at Contractor’s expense) so that a Federal Criminal Background Check may be completed by DTS, at DTS’s expense. DTS will provide Contractor with forms which must be filled out by Contractor and returned to DTS. Each employee of Contractor or a Subcontractor who will have Access to Secure State Facilities, State Data, or Technology must be fingerprinted by DTS or local law enforcement a minimum of one week prior to needing access. At the time of fingerprinting, said employee shall disclose all felony or misdemeanor convictions. DTS will conduct a Federal Criminal Background Check based upon the fingerprints and personal information provided and use this same information to complete a Name Check in the Utah Criminal Justice Information System (UCJIS) at least every two years. Contractor and the employee or Subcontractor shall immediately notify DTS if an arrest or conviction for a felony or misdemeanor of any person that has Access to Secure State Facilities, State Data or Technology occurs during the Contract Period. Additionally, each employee, consultant of Contractor, and Subcontractor who will be granted unescorted access to Secure State Facilities, State Data, or Technology must successfully complete a 10-panel drug test at Contractor’s expense with the pass/fail results of the drug test provided to the State of Utah’s hiring manager prior to such access being granted. DTS may revoke Access to Secure State Facilities, Data, and Technology in the event the results of a drug test are positive. DTS will determine in its discretion if such person’s Access to Secure State Facilities, State Data, or Technology shall remain in effect. Contractor’s employees and any Subcontractors who have unescorted Access to Secure State Facilities or to State or Federal Data or any Access to Technology will complete at no additional cost any required security training as requested by the State. Felony and misdemeanor are defined by the laws of the State of Utah, regardless of where the conviction occurred.
2. **SECURE PROTECTION AND HANDLING OF STATE DATA:** If Contractor is given access to or will be storing State Data, the protection of State Data shall be an integral part of the business activities of Contractor, and Contractor shall ensure that there is no inappropriate or unauthorized use of State Data. Contractor shall safeguard the confidentiality, integrity, and availability of the State Data and comply with the conditions outlined below. DTS reserves the right to verify Contractor’s adherence to the following conditions to ensure they are met:
	1. **Network Security**: Contractor shall maintain network security that, at a minimum, includes: network firewall provisioning, intrusion detection, and regular third-party penetration testing. Contractor shall maintain network security and ensure that Contractor network security policies conform to the following:
		1. The Current standards set forth and maintained by the National Institute of Standards and Technology in SP 800-53 found at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final; and
		2. All applicable FedRAMP or GovRAMP security requirements, including but not limited to, continuous monitoring, incident response, and data classification as outlined in GovRAMP documentation.
	2. **State Data Security:** Contractor shall protect and maintain the security of State Data with protection that is at least as good as or better than that maintained by the State of Utah as identified in *DTS Policy 5000-0002*. These security measures include but are not limited to maintaining secure environments that are patched and up to date with all appropriate security updates as designated (ex. Microsoft Notification). Data access must incorporate the principles of least privilege and be physically and technologically controlled. DTS reserves the right to determine if Contractor’s level of protection meets the State’s security requirements.
	3. **State Data Transmission**: Contractor shall ensure all transmission or exchange of system application data with the State of Utah and/or any other parties expressly designated by the State of Utah, shall be encrypted and take place via secure means (ex. HTTPS or FTPS). Transmission of regulatory data must conform with the current regulatory requirement applicable to such data (ex. FIPS 140-x).
	4. **State Data Storage**: All State Data will be stored and maintained in data centers in the United States. State Data is required to be encrypted in transit and at rest. State Data may only be processed on or transferred to Contractor-owned portable or laptop computing device or portable storage medium if such device is whole disk encrypted, or used and kept only at Contractor’s United States data centers, including if such medium is part of the Contractor's designated backup and recovery process. IN NO CASE MAY SUCH DEVICES OR STATE DATA LEAVE THE UNITED STATES.
	5. **Access**: Contractor may permit its employees and Subcontractors to remotely access non-State Data as required to provide technical support.
	6. **State Data Encryption**: Contractor shall store all data provided to Contractor, including State Data, as well as any backups made of that data, in encrypted form based on the current TLS standard and include all data as part of a designated backup and recovery process. Encryption of regulatory data must conform with the current regulatory requirement applicable to such data (ex. FIPS 140-x).
	7. **Authentication**: Any portable or laptop computer that has access to State of Utah resources shall be equipped with strong and secure password protection. All systems that require authentication must use the Single Sign On solution operated by the State of Utah. This may be accomplished through federation using standard authentication protocols or direct integration into the vendor supplied application. If the Goods or Services, or both, are to be accessed or used by both Internal (state employees, contractors, etc.) and External (public, etc.) users, then the Goods and Services must be able to be integrated with multiple identity providers at the same time.
	8. **Confidential Information Certification:** Contractor may be required to sign a Confidential Information Certification form prior to being given access to certain confidential computerized records, if required by agency or Federal policies.
	9. **State Data Re-Use:** All data exchanged shall be used expressly and solely for the purpose enumerated in this Contract. No State Data of any kind may be transmitted, exchanged, or provided to other contractors or third parties except on a case-by-case basis as specifically agreed to in writing by the State Entity.
	10. **State Data Destruction**: No sooner than 60 days but no later than 90 days following the expiration or termination of this Contract and only after ensuring compliance with Section 20 (Ownership, Protection, and Return of Documents and Data) of this Attachment B, Contractor shall erase, destroy, and render unreadable all State Data from all non-state computer systems and backups, and certify in writing that these actions have been completed within one hundred twenty (120) days of the expiration or termination of this Contract or within seven (7) days of the request of the State Entity, whichever shall come first, unless the State Entity provides Contractor with a written directive otherwise. The State Entity’s written directive may require that certain data be preserved in accordance with applicable law.
	11. **Services Shall Be Performed Within the United States**: All Non-Public Data, including Criminal Justice Information (CJI), Personally Identifiable Information (PII), and other sensitive data, must be stored, processed, and disposed of within the United States. Contractor is prohibited from transferring, storing, or accessing Non-Public and/or State Data outside the United States without explicit written authorization from the State of Utah via an approved exception request from the Chief Information Security Officer (CISO) and must be documented in the system security plans of such systems, with a description of any compensating controls and a business justification. Offshore support is only permitted for systems not using Non-Public Data. Contractor must provide a list of countries and Subcontractors from which Services will be provided to ensure no undue risk to State Data and systems.
	12. **Federal Data Protection:** Contractor must store all Federal Data in a manner that, at all times, is physically and electronically secure from access by unauthorized persons. Contractor must employ both physical and technological barriers to prevent unauthorized retrieval of Federal Data via computer, remote terminal, or other means. Federal Data must be subject to separation-of-duties protocols and provided only to those with a need to know.
		1. Each query for Federal Data in Contractor’s system (including read-only and system access events that do not result in a change to data or a new transaction) must be stored as a separate record, not overlaid by subsequent records. All viewing of Federal Data must be recorded by a fully-automated audit trail system, which can be via an online query, automated report, batch processing, or any other logical means. Access to the audit file must be restricted to authorized users with a need to know and be maintained for a minimum of three years or the amount of time required by a federal agency, whichever is greater.
		2. Contractor must delete, purge, destroy, or return to the State of Utah all Federal Data upon termination of the Contract with no output to be retained by Contractor. If immediate purging is not possible, Contractor will certify that any Federal Data in physical or electronic storage will remain safeguarded to prevent unauthorized disclosure. Contractor agrees to abide by all relevant federal laws, restrictions on access, use, disclosure, and security requirements in the State’s data exchange agreement with the social security administration. If applicable, Contractor will permit the State to conduct, at least once every three years and upon prior notice, a review to verify that the Contract is in compliance with the State’s agreement with the social security administration.
		3. Federal Data shall be used only for the purpose of carrying out the provisions of the Contract. Federal Data shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract.
		4. All computer systems receiving, processing, storing, or transmitting Federal Data must meet the requirements set forth by the applicable federal agency.
3. **LIABILITY FOR SECURITY INCIDENT OR DATA BREACH.** In the event of a Security Incident or Data Breach, liability for notification and remedial costs and damages shall be the responsibility of the party who controls how the data is processed.
4. **SECURITY INCIDENT OR DATA BREACH NOTIFICATION:** As required by Utah Code 63A-19-405 or any other applicable data breach reporting laws, upon discovery of any Security Incident or Data Breach or privacy breach of Personal Data (including loss of access to Personal Data), Contractor shall provide the notification to the State Entity and DTS in the most expedient time possible without unreasonable delay. Contractor shall adhere to all applicable data breach reporting laws and will, upon the State of Utah’s request, provide Contractor’s incident response plans to the State of Utah. It is within DTS’s discretion to determine whether any attempted unauthorized access is a Security Incident or a Data Breach.
5. **Incident Response**: Contractor may need to communicate with outside parties regarding a Security Incident or a Data Breach, which may include contacting law enforcement and seeking external expertise as mutually agreed upon, defined by law, or contained in this Contract. Discussing Security Incidents or Data Breaches with DTS must be handled on an urgent as-needed basis, as part of Contractor’s communication and mitigation processes.
6. **Incident Reporting Requirements**: Contractor shall promptly report a Security Incident or Data Breach to DTS and the State Entity. DTS may be contacted in one of the following ways:

E-mail - DTS-SOC@utah.gov

Phone – (801) 538-3011

Web - [cybercenter.utah.gov](http://cybercenter.utah.gov/)

1. **SECURITY INCIDENT OR DATA BREACH RESPONSIBILITIES:** Contractor shall comply with all applicable laws that require the notification of individuals in the event of a Security Incident or Data Breach, or other events requiring notification in accordance with DTS Policy 5000-0002 Enterprise Information Security Policy. In the event of a Security Incident or Data Breach requiring notification under Utah Code § 63A-19-405 and 406, Contractor shall: (a) cooperate with DTS by sharing information relevant to the Security Incident or Data Breach; (b) promptly implement necessary remedial measures; and (c) 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 relation to the Security Incident or Data Breach. If the Data Breach requires public notification, all communication shall be coordinated with DTS.
2. **COMPLIANCE WITH NIST 800.53** If Contractor is developing software for the State or providing Goods or Custom Deliverables or performing Services which have the potential to cause any form of outage or to modify any State of Utah infrastructure, Contractor shall comply with current standards set forth and maintained by the National Institute of Standards and Technology, NIST 800-53 (Rev 5 or current version) and/or GovRAMP or FedRAMP for cloud solutions, as applicable. If Contractor fails to maintain or achieve the security requirements outlined above, the Contractor may be subject to liquidated damages and/or the State of Utah may determine whether the failure to comply justifies Contract termination. If an amount of liquidated damages is specified in the Contract, that will be the limit for said damages, or if an amount is not specified, then at the discretion of the State of Utah, when declaring a default, the State of Utah may specify the amount of liquidated damages up to, or capped at, the total amount paid to the Contractor up until the date of the default.
3. **USE OF AI OR STATE SUB DOMAIN:** Contractor must inform the State of Utah of any Generative Artificial Intelligence (“GenAI”) in the Goods or Services being contracted for prior to providing those Goods or Services to the State. Additionally, utilization of GenAI in the creation of Goods and Services impacting the State’s Intellectual Property Rights shall include annotations sufficient to comply with DTS POLICY 4000-0008 Enterprise Generative AI Policy.
4. Contractor is prohibited from using State Data for building or training GenAI programs without prior written permission from the State. Contractor attests that its GenAI models use only properly licensed material. Should Contractor be found in violation of this requirement, Contractor shall fully indemnify and defend the State of Utah from all claims related thereto. Furthermore, should Contractor learn that State Data has been used in GenAI queries without permission from the State of Utah, Contractor shall immediately notify the State of Utah of the use and cover the full expense of any remediation.
5. Contractor shall support usage of a utah.gov subdomain according to R895-4 for Goods and Services that will be made available to non-state users.
6. Contractor is prohibited from using, integrating, or otherwise conjoining Personal Data with GenAI in any way and under any circumstances.
7. **CONFIDENTIALITY:** If Contractor’s Subcontractors have access to or process Personal Data, Contractor shall advise the Subcontractor of the obligations required under this Contract to keep all Personal Data strictly confidential, and advise the Subcontractor to comply with any requirements contained in the Contract such as permitted uses, disclosures, handling, and destruction of Personal Data. Some privacy and data protection laws may require disclosure of Subcontractors who process State Data that includes Personal Data.
8. **BUSINESS ASSOCIATE AGREEMENT:** If the nature of the parties’ interactions is such that PHI will be exchanged, the parties will negotiate a Business Associate Agreement in good faith.
9. **UTAH CODE 63G-6a-1203:** Contractor acknowledges that those contractual provisions identified in Utah Code 63G-6a-1203 as void and unenforceable are, in fact, void and unenforceable, even if such provisions are found in this Contract, with the possible exception of 63G-6a-1203 (4)(f) and 4(i), in which cases legal counsel for the specific procurement unit must have made an exemption in accordance with subsection (5) and/or (6).

 (Revision Date: 1 July 2025)