

ATTACHMENT I

Information Resources and Security Requirements

1. TYPES OF DATA

“**TxDOT Data**” means TxDOT information, data, records, and information to which a Contractor-Related Entity has access, has possession, or is otherwise provided to a Contractor-Related Entity by TxDOT, whether or not intended under or for the purposes of the agreement, including, without limitation, data generated or collected under this agreement, intellectual property created as a work for hire under this agreement, and Personal Identifying Information (as defined below).

TxDOT Data is classified into the four categories that control applicability of security standards: Public, Sensitive, Confidential, and Regulated. See Section 4 for Definitions.

Any data that a Contractor-Related Entity accesses and downloads from a TxDOT system, for use, manipulation, storage, or management is considered Confidential Data unless otherwise specified in writing by TxDOT.

2. DATA REQUIREMENTS

2.1 Data, Data Dictionaries, and Data Flow Diagrams

Contractor shall ensure that all TxDOT Data that is generated, manipulated, transmitted, or stored, utilizes the TxDOT taxonomy, with documented data dictionaries, and data flow diagrams (including security protocols).

2.2 Data Transfer

- (a) At the completion of a deliverable, the Contractor shall transfer all TxDOT Data generated and stored for that deliverable to TxDOT in a manner and format acceptable to TxDOT and approved by TxDOT’s Information Technology Division (“**ITD**”).
- (b) All metadata associated with the TxDOT Data transferred must remain attached to that data.
- (c) Contractor shall maintain the appropriate level of data security throughout the transfer of the TxDOT Data.

2.3 Backup and Disaster Recovery

- (a) Contractor shall implement business continuity procedures to fulfill all requirements of this agreement that address, as a minimum, fire, theft, natural disaster, technical difficulty, workforce problems equipment failure, or other disruption of business.
- (b) Contractor shall maintain a disaster recovery plan. Contractor is responsible for all project related costs of disaster recovery during the project except for costs associated with disasters beyond Contractor’s reasonable control, and for those costs included as part of the TxDOT infrastructure responsibilities.

2.4 Open Records Requests

Contractor shall not release Information in response to an open record request related to this agreement request unless TxDOT has approved the release in writing.

2.5 Encryption

For Sensitive, Confidential, and Regulated TxDOT Data, the Contractor shall ensure TxDOT Data is encrypted while in-transit and while at-rest in accordance with the TxDOT Controls Catalog Standard SC-13, Cryptographic Protection and SC-08, Transmission Confidentiality and Integrity security requirements.

2.6 Accessibility

Contractor shall ensure all products provided under this agreement comply with the State of Texas Accessibility requirements for Electronic and Information Resources specified in 1 Texas Administrative Code (TAC) Chapters 206 and 213.

3. INFORMATION RESOURCE AND SECURITY REQUIREMENTS

3.1 Information Security Safeguards

- (a) Contractor shall implement appropriate administrative, physical, and technical safeguards, in accordance with TxDOT's security requirements, that reasonably and appropriately protects the confidentiality, integrity, and availability of TxDOT Data.
- (b) Contractor shall conform its policies and procedures relating to the implementation of security safeguards to comply with TxDOT's Information Resources security program pursuant to the TxDOT and DIR's Information Security Controls Catalog Standards.

3.2 Potential Cybersecurity Incident or Breach Notification

Contractor shall immediately report to TxDOT via the Report Cybersecurity Incident Page on TxDOT.gov, any potential cybersecurity incident or breach involving TxDOT Data (See Section 4, Definitions).

3.3 Demonstrating Compliance with Information Security Requirements

If required by TxDOT, prior to contract award, at renewal, and on a recurring basis, Contractor shall provide a TxDOT Security Questionnaire as documented in the contract. Additionally, upon reasonable notice to the Contractor, and if TxDOT determines that the Contractor has violated this agreement, TxDOT, directly or through its agent, may request an attestation, which may include additional attestations, and evidence that Contractor is in compliance with applicable laws, regulations, and standards outlined in 3.5.

3.4 Security Training

In accordance with Section 2054.5192 of the Texas Government Code, each Contractor-Related Entity that will access a TxDOT computer system or database must complete a TxDOT approved cybersecurity training program that is certified under Section 2054.5192 of the Texas Government Code. The training program must be completed during the term of the contract and during any renewal period. The Contractor shall provide verification of completion of the cybersecurity training program in a method designated by TxDOT.

3.5 Applicable Laws, Regulations, and Standards

Contractor shall perform the services in accordance with the following standards, notify TxDOT of situations where compliance is not achievable, and assist TxDOT with the prevention of security gaps or conflicts that could impair security performance. Contractor shall comply with all applicable federal, state, and local laws and regulations necessary to perform the services. A non-exhaustive list of federal, state, and local laws and regulations that might be applicable includes the following.

- (1) DIR Security Controls Standard Catalog and applicable TxDOT Security Requirements
 - (A) For Public Data, TxDOT and DIR Security Controls Standards Catalog low baseline and applicable TxDOT security requirements.
 - (B) For Sensitive Data TxDOT and DIR Security Controls Standards Catalog low baseline with Sensitive overlay and applicable TxDOT security requirements.
 - (C) For Confidential Data, TxDOT and DIR Security Controls Standards Catalog moderate baseline and applicable TxDOT security requirements.
 - (D) For Regulated Data, TxDOT and DIR Security Controls Standards Catalog moderate

baseline, applicable TxDOT security requirements, and applicable regulated security requirements.

- (2) TX-RAMP Requirements
 - (A) Contractor shall ensure that any Contractor-Related Entities providing a Cloud Computing Service to TxDOT that creates, accesses, transmits, uses, or stores TxDOT Data must be authorized in the Texas Risk and Authorization Management Program (“**TX-RAMP**”) if TxDOT determines TX-RAMP is required.
 - (B) TxDOT may approve the use of a TX-RAMP provisional status in lieu of a TX-RAMP certification. This approval is not effective unless approved in writing by the TxDOT Chief Information Security Officer (“**CISO**”) and DIR.
 - (C) Applicable Contractor-Related Entities must achieve the following levels of authorization by the following dates for any new contract or renewal of existing contract:
 - a. TX-RAMP Level 1 Status no later than January 1, 2024
 - b. TX-RAMP Level 2 Status no later than January 1, 2022
- (3) State Laws and Regulations:
 - (A) Texas Administrative Code, Chapter 202 – Information Security Standards
 - (B) Texas Administrative Code, Chapter 206 – State Websites
 - (C) Texas Administrative Code, Chapter 213 – Electronic and Information Resources
 - (D) Texas Government Code, Chapter 552 – Public Information
 - (E) Texas Government Code, Chapter 2054 – Information Resources
 - (F) Texas Penal Code, Chapter 33 – Computer Crimes
 - (G) For Confidential data, Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information
 - (H) For Confidential data containing Protected Health Information, Texas Health and Safety Code, Chapter 181 – Medical Records Privacy
 - (I) For Regulated data containing Payment Card Industry (“**PCI**”) information, the Payment Card Industry Data Security Standards (“**PCI-DSS**”)
 - (J) For Regulated data containing Criminal Justice Information (“**CJI**”), the Criminal Justice Information Services (“**CJIS**”) Security Policy

3.6 Information Resources Technology

- (a) Any proposed information resources technology that will be installed on any TxDOT owned equipment or that will access any TxDOT network must be reviewed and approved by the ITD Architectural Review Board (“**ARB**”) prior to any development or design.
- (b) Any proposed information resources technology that will be installed on any TxDOT owned equipment or that will access any TxDOT network must be reviewed and approved by the ITD Change Advisory Board (“**CAB**”) prior to implementation or delivery.

3.7 Information Resources Technology (“**IRT**”) Procurements

ITD must approve all procurements of:

- (1) Information Resources Technology that will be owned by TxDOT.
- (2) IT services for any environment that provides processing, storage, networking, management and the distribution of data to ensure alignment with Texas Government

Code, Chapter 2054, Subchapter L.

3.8 Prohibited Technologies

In accordance with the Texas Statewide Plan for Prohibited Technologies, Contractor shall not provide services, equipment, or systems to TxDOT determined to be a Prohibited Technology by TxDOT. A list of the entities currently determined to be Prohibited Technologies is available at:

<https://ftp.txdot.gov/pub/txdot/itd/cybersecurity/prohibited-technologies-list-cybersecurity.pdf>

3.9 Background Checks Required for Access to TxDOT Data and TxDOT Systems

- (a) The contractor shall ensure that a Background Check is performed on each Contractor-Related Entity prior to that person receiving access to any TxDOT system.
- (b) Contractor shall ensure that a Background Check is performed on each Contractor-Related Entity prior to that person receiving access in a Contractor-Related Entity Environment to TxDOT Data that requires a Moderate or High Security Baseline
- (c) A “**Background Check**” must include the following:
 - (1) Verification of Social Security number;
 - (2) All true alias names and counties
 - (3) Federal and county level checks for felony and misdemeanor arrest and convictions for the past seven years, including sentences of deferred adjudication – all names;
 - (4) Search of national criminal database – all names;
 - (5) Search of state and national sex offender registry – all names; and
 - (6) Search of the government sanction registry listings.
- (d) Contractor shall not allow any Contractor-Related Entity for which Contractor received any unfavorable result when conducting a Background Check to access TxDOT Data or any TxDOT System.
- (e) TxDOT may make exceptions to 3.9(d) on a case-by-case basis. Any exception granted by TxDOT must be in writing to be effective.
- (f) Upon request by TxDOT, Contractor shall provide documentation that demonstrates to TxDOT’s satisfaction that Background Checks have been conducted as required and that no Contractor-Related Entity with one or more unfavorable results has received access to TxDOT Data or any TxDOT System.
- (g) Contractor shall immediately notify TxDOT if it learns of any change in status that might cause a Contractor-Related Entity to receive an unfavorable result from a Background Check.
- (h) If Contractor fails to meet the requirements of 3,9, TxDOT may terminate this contract immediately with no further liability to the Contractor.

3.10 Interconnection of TxDOT and Contractor-Related Entity Environment

If a Contractor-Related Entity has or will have one or more interconnections between an Information System in that Contractor-Related Entity’s Environment and a TxDOT System or Systems, the Contractor shall execute or cause to be executed an Interconnection Security Agreement (“**ISA**”) for each interconnection. An executed ISA must be provided to TxDOT for each new interconnection prior to connection.

- 3.11 Upon request by TxDOT, the Contractor shall provide any additional information or documentation that TxDOT determines is necessary to confirm a Contractor-Related Entity’s compliance with this section. If Contractor fails to provide requested information as required, TxDOT may terminate this contract immediately with no further liability to the Contractor.

3.12 If completion of any of the requirements in this section requires obtaining information and/or action from a Contractor-Related Entity or other non-party entity, Contractor shall obtain the required information or action from that entity. For example, if the Contractor is a reseller of a Contractor-Related Entity's product or service, the Contractor is responsible for completing the TxDOT Security Questionnaire and the Contractor must obtain all the information or actions from the Contractor-Related Entity necessary for the Contractor to complete the questionnaire.

3.13 SOC 1 Type 2 and SOC 2 Type 2 Requirements

If a Contractor-Related Entity is determined to be providing a function that is a key internal financial control or has a material financial impact on the TxDOT financial statements, then the following are applicable:

- (a) Provide an Annual Report – Contract-Related entity must provide TxDOT the audit SSAE 18 Results within 15 days of Contract-Related receipt of final report from independent auditor. Licensor will engage a third party (the "Service Provider") to conduct an examination in accordance with Statement on Standards for Attestation Engagements No. 18, as established by the American Institute of Certified Public Accountants (AICPA), and commonly referred to as a Service Organization Controls (SOC) 1, relevant to controls related to the solution, and prepare a SOC 1 Type 2 report with respect thereto (the "SOC 1 Report").
- (b) In addition, Licensor will engage a Service Provider to conduct an examination in accordance with AT Section 101 of the Statement on Standards for Attestation Engagements to report on controls at a Service Organization relevant to security and availability, established by the AICPA ("AICPA Standards") and, subject to AICPA Standards, prepare a Type 2 service organization controls report with respect thereto (the "SOC 2 Report"). Once the SOC 1 Report and SOC 2 Report are each available, upon written request from Licensee, Licensor must make available Licensor personnel to discuss with TxDOT the reports. Other report types will not be considered to meet these requirements.

4. DEFINED TERMS

- 4.1 "**baseline**" means the set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system. Information on applicable baselines is available at <https://www.txdot.gov/inside-txdot/division/information-technology/Cybersecurity/cybersecurity-resources.html>.
- 4.2 "**Breach**" means "breach of system security" as defined in Section 521.053(a) of the Texas Business and Commerce Code, which defines breach of system security as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."
- 4.3 "**Cloud Computing Service**" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is referenced in Texas Government Code Title 10, Subtitle D, Chapter 2157, Subchapter A, Section 2157.007 and is defined in NIST 800-145.
- 4.4 "**Confidential Information**" has the meaning provided in 1 Texas Administrative Code § 202.1(5), which states the confidential information means "information that must be protected from unauthorized disclosure or public release based on published laws or legal agreements." Information that is Confidential Information under this definition includes:
 - (a) Dates of birth of living persons
 - (b) Driver's license numbers

- (c) License plate numbers
 - (d) Credit card numbers
 - (e) Insurance policy numbers
 - (f) Attorney-Client communications
 - (g) Drafts of policymaking documents
 - (h) Information related to pending litigation
 - (i) Audit working papers
 - (j) Competitive bidding information before contract awarded.
 - (k) Personal Identifiable Information
 - (l) Sensitive Personal Information
 - (m) Regulated data
 - (n) Information excepted from disclosure requirements of Chapter 552 of the Texas Government Code (“**Texas Public Information Act**”) or other applicable state or federal law
 - (o) Compliance reports for which the Texas Attorney General has granted permission to withhold
 - (p) Investigative working papers and draft reports excepted from disclosure under Section 552.116 of the Texas Government Code
- 4.5 “**Contractor-Related Entity**” means Contractor; subcontractors; their employees, agents and officers; and all other persons for whom Contractor might be legally or contractually responsible.
- 4.6 “**Contractor-Related Entity Environment**” means an Environment for which TxDOT does not manage or control the system environment, servers, operating systems, or storage with the exception of user-specific configuration settings.
- 4.7 “**Data**” means the representation of facts; as the raw material of information that is used as a basis for reasoning, decision-making, discussion, or calculation.
- 4.8 “**Data Dictionary**” means a directory of the definitions, purpose, policies and structure about data. It is a compilation of information about the data owned by the enterprise. It describes every data item in a database in enough detail for users and application developers to know what the data is and how to make use of it.
- 4.9 “**Environment**” means an aggregate of procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.
- 4.10 “**Information**” means data, regardless of form, that is created, contained in, or processed by information resources facilities, communications networks, or storage media.
- 4.11 “**Information Resources Technology**” means data processing and telecommunications hardware, software, services, supplies personnel, facility resources, maintenance and training that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.
- 4.12 “**Information System**” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. An Information System normally includes, but is not limited to, hardware, software, network infrastructure, information, applications, communications, and people.
- 4.13 “**Personal Identifying Information**” means information that alone or in conjunction with other information identifies an individual, including an individual's:

- (a) Name, social security number, date of birth, or government-issued identification number;
 - (b) Mother's maiden name;
 - (c) Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; and
 - (d) Unique electronic identification number, address, or routing code.
- 4.14 **“Potential Cybersecurity Incident”** means an event which may result in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.
- 4.15 **“Public Data”** means Data that is subject to public disclosure pursuant to the Texas Public Information Act and freely and without reservation made available to the public.
- 4.16 **“Public information”** means information written, produced, collected, assembled, or maintained by or for a governmental body, including information held by individual officers or employees of a governmental body, in connection with the transaction of official TxDOT business. This includes information that is held by contractors and consultants and that TxDOT owns, to which TxDOT has a right of access, or on which public money was spent for the purpose of writing, producing, collecting, assembling, or maintaining the information. Public information includes any electronic communication created, transmitted, received, or maintained on any device if the communication is in connection with the transaction of official business. Public information may be stored in any medium and may exist in forms such as books, papers, letters, documents, e-mails, Internet postings, text messages, instant messages, printouts, photographs, maps, drawings, and audio and video recordings. Public information does not include tangible items, such as computers or guardrails.
- 4.17 **“Regulated Data”** means information for which the use and protection of is dictated by a state or federal agency or by third party agreements.
- 4.18 **“Sensitive Data”** means information that could be subject to release under an open records request, but should be controlled to protect third parties, and should be vetted and verified before release. At TxDOT, this could include operational information, personnel records, research, or internal communications.
- 4.19 **“Sensitive Personal Information”** has the meaning provided by Section 521.002(2) of the Texas Government Code, which defines sensitive personal information as:
- (a) An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and item are not encrypted:
 - (1) Social Security Number
 - (2) Driver’s license number or government-issued identification number; or
 - (3) Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or
 - (b) Information that identifies an individual and relates to:
 - (1) The physical or mental health or condition of the individual;
 - (2) The provision of health care to the individual; or
 - (3) Payment for the provision of health care to the individual.
- 4.20 **“TxDOT Security Questionnaire”** means a cybersecurity and privacy questionnaire that provides TxDOT ITD necessary information for third party attestation in accordance with TxDOT requirements.

4.21 **“TxDOT System”** means an Information System that is owned, managed, or maintained by TxDOT or on behalf of TxDOT.