1. Types of Data

“TxDOT Data” means TxDOT information, data, records, and information to which the Contractor has access, has possession, or is otherwise provided to the Contractor 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 three categories that control applicability of security standards: Confidential, Sensitive, and Public. See Section 4 for Definitions.

Any data that the Contractor accesses and downloads from a TxDOT system, for use, manipulation, storage, or management is 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

2.2.1. At the completion of a deliverable, the Contractor shall transfer all TxDOT Data generated and stored for that deliverable to State in manner and format acceptable to the State and approved by IMD.

2.2.2. All metadata associated with the TxDOT Data transferred must remain attached to that data.

2.2.3. Contractor shall maintain the appropriate level of data security throughout the transfer of the TxDOT data.

2.3. Backup and Disaster Recovery

2.3.1. 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.

2.3.2. 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

2.4.1. 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 and Confidential TxDOT data, the Contractor shall encrypt the data while in-transit and while at-rest in accordance with the Department of Information Resources (“DIR”) Controls Catalog Standard SC-13, Cryptographic Protection and SC-08, Transmission Confidentiality and Integrity and TxDOT security requirements.

3. Information Resource and Security Requirements
3.1. **Information Security Safeguards**

3.1.1. 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.

3.1.2. 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 Texas Department of Information Resources’ Information Security Controls Catalog Standards. Systems with Public data must be in compliance with the low baseline and systems with Sensitive and Confidential data must be compliant with the moderate baseline.

3.2. **Breach Notification**

Contractor shall immediately report to TxDOT via IMD-Security@TxDOT.gov any security breach of TxDOT data that the Contractor is responsible for (See Section 4, Definitions).

3.3. **Demonstrating Compliance with Information Security Requirements**

Upon reasonable notice to the Contractor, or if TxDOT determines that the Contractor has violated this agreement, TxDOT, directly or through its agent, may request an attestation and evidence that Contractor is in compliance with applicable laws, regulations, and standards outlined in 3.4.

3.4. **Security Training**

3.4.1. In accordance with Section 2054.519 of the Texas Government Code, each Contractor Personnel that will access a TxDOT computer system or database must complete a TxDOT approved cybersecurity training program that is certified under Section 2054.519 of the Texas Government Code. The training program must be completed by each Contractor Personnel 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.

3.4.2. In this section, “Contractor Personnel” includes officers and employees of both the Contractor and its subcontractors.

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 include the following.

3.5.1. DIR Security Controls Standard Catalog and applicable TxDOT Security Requirements

3.5.1.1. For Public Data, Texas DIR Security Controls Standards Catalog low baseline and applicable TxDOT security requirements

3.5.1.2. For Sensitive and Confidential Data, Texas DIR Security Controls Standards Catalog moderate baseline and applicable TxDOT security requirements.

3.5.2. State Laws and Regulations:

3.5.2.1. Title 1 of Texas Administrative Code

3.5.2.1.1. Chapter 202 – Information Security Standards

3.5.2.1.2. Chapter 206 – State Websites

3.5.2.1.3. Chapter 213 – Electronic and Information Resources

3.5.2.2. Texas Government Code, Chapter 552 – Public Information

3.5.2.3. Texas Penal Code, Chapter 33 – Computer Crimes

3.5.2.4. For Confidential data, Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information
3.5.2.5. For Confidential data containing Protected Health Information, Texas Health and Safety Code, Chapter 181 – Medical Records Privacy

3.6. **Information Resources Technology**

3.6.1. 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 Architectural Review Board ("ARB") in the Information Management Division ("IMD") prior to any development or design.

3.6.2. 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 IMD Change Advisory Board ("CAB") prior to implementation or delivery.

3.7. **Information Resources Technology ("IRT") Procurements**

IMD must approve all procurements of:

3.7.1. Information Resources Technology that will be owned by TxDOT.

3.7.2. IT services for any environment that provides processing, storage, networking, management and the distribution of data to ensure alignment with GAC, Chapter 2054, Subchapter L.

4. **DEFINED TERMS**

4.1. **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.”

4.2. **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

4.2.1. Dates of birth of living persons

4.2.2. Driver’s license numbers

4.2.3. License plate numbers

4.2.4. Credit card numbers

4.2.5. Insurance policy numbers

4.2.6. Attorney-Client communications

4.2.7. Drafts of policymaking documents

4.2.8. Information related to pending litigation

4.2.9. Audit working papers

4.2.10. Competitive bidding information before contract awarded.

4.2.11. Personal Identifiable Information

4.2.12. Sensitive Personal Information

4.2.13. Regulated data

4.2.14. Information excepted from disclosure requirements of Chapter 552 of the Texas Government Code ("Texas Public Information Act") or other applicable state or federal law

4.2.15. Compliance reports for which the Texas Attorney General has granted permission to withhold

4.2.16. Investigative working papers and draft reports excepted from disclosure under Section 552.116
4.3. "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.

4.4. "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.

4.5. "Information" means data, regardless of form, that is created, contained in, or processed by information resources facilities, communications networks, or storage media.

4.6. "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.

4.7. "Personal Identifying Information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

   4.7.1. Name, social security number, date of birth, or government-issued identification number;
   4.7.2. Mother's maiden name;
   4.7.3. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
   4.7.4. Unique electronic identification number, address, or routing code; and

4.8. "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.

4.9. "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.

4.10. "Sensitive Data" means any information that could be subject to release under an open records requests, 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.

4.11. "Sensitive Personal Information" has the meaning provided by Section 521.002(2) of the Texas Government Code, which defines sensitive personal information as:

   4.11.1. 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:

       4.11.1.1. Social Security Number
       4.11.1.2. Driver's license number or government-issued identification number; or
4.11.1.3. 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

4.11.2. Information that identifies an individual and relates to:

   4.11.2.1. The physical or mental health or condition of the individual;

   4.11.2.2. The provision of health care to the individual; or

   4.11.2.3. Payment for the provision of health care to the individual.