

Information Resources and Security Requirements

1. PURPOSE AND INTRODUCTION

1.1.

In the course of performing Work under the Agreement, Vendor may gain access to TxDOT Data (defined below). In this event, TxDOT and Vendor desire to appropriately protect TxDOT Data. The purpose of these Information Resources and Security Requirements are to specify Vendor's cybersecurity and risk management responsibilities when Vendor has access to TxDOT Data.

1.2.

Vendor agrees to provide enterprise-grade cybersecurity and risk management to protect TxDOT Data, as further described and set forth herein.

2. TYPES OF DATA

As described below, TxDOT Data is classified into four categories that control applicability of security standards: Public, Sensitive, Confidential, and Regulated.

Vendors accessing, transmitting, storing, or using TxDOT Data must comply with the appropriate security requirements as set forth in the TxDOT Information Security and Privacy Controls Standard Catalog (the "Catalog"), available on the [Cybersecurity Resources](#) page.

3. DATA REQUIREMENTS

3.1. Data, Data Dictionaries, and Data Flow Diagrams

Vendor shall ensure that all TxDOT Data that is generated, manipulated, transmitted, or stored by Vendor utilizes the TxDOT taxonomy, with

documented data dictionaries and data flow diagrams (including security protocols).

3.2. Data Transfer

- a) At the completion of a deliverable, Vendor 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) Vendor shall maintain the appropriate level of data security throughout the transfer of the TxDOT Data.

3.3. Backup and Disaster Recovery

- a) Vendor 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) Vendor shall maintain a disaster recovery plan. Vendor is responsible for all project related costs of disaster recovery during the project except for costs associated with disasters beyond Vendor's reasonable control, and for those costs included as part of the TxDOT infrastructure responsibilities.

3.4. Encryption

For Sensitive, Confidential, and Regulated TxDOT Data, Vendor shall ensure TxDOT Data is encrypted while in-transit and while at-rest in accordance with the Catalog Standards SC-08, Transmission Confidentiality and Integrity Security Requirements, SC-13, Cryptographic Protection, and SC-28, Protection of Information at Rest.

3.5. Accessibility

Vendor shall ensure all products provided under the Contract comply with the State of Texas accessibility requirements for electronic and information resources specified in 1 Texas Administrative Code (TAC) chapters 206 and 213, as applicable.

3.6. Data Location

Irrespective of any other provision of the Contract or its incorporated or referenced documents, all TxDOT Data shall remain, and be stored, processed, accessed, viewed, transmitted, and received, always and exclusively within the contiguous United States.

3.7. Data Destruction

Upon expiration or termination of the Contract, after Vendor transfers all TxDOT Data to TxDOT in a manner and form specified by TxDOT and TxDOT confirms receipt of data, TxDOT Data within the Vendor's environment must be removed and sanitized unless retention is explicitly authorized by TxDOT in writing.

4. INFORMATION RESOURCE AND SECURITY REQUIREMENTS

4.1. Information Security Safeguards

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

4.2. Cybersecurity Incident or Breach Notification

Vendor shall immediately report to TxDOT via the Report Cybersecurity Incident Page on TxDOT.gov, any Cybersecurity Incident or Breach involving TxDOT Data.

4.3. Demonstrating Compliance with Information Security Requirements

Vendor shall provide a current TxDOT Security Questionnaire to TxDOT within 5 business days of a request. Additionally, upon reasonable notice to Vendor, and if TxDOT determines that Vendor has violated the data security requirements set forth herein, TxDOT may request a written attestation and supporting evidence demonstrating compliance with the requirements set forth herein.

4.4. Security Training

In accordance with Section 2063 of the Texas Government Code, each Vendor that will access a TxDOT computer system or database must complete a TxDOT-approved cybersecurity program that is certified under Section 2063.104 of the Texas Government Code. The training program must be completed during the term of the Contract and during any renewal period. Vendor shall provide verification of completion of the cybersecurity training program in a method designated by TxDOT.

4.5. Standards

- 1) Vendor shall perform the Work in accordance with the following standards. Vendor shall 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.
 - A) For Public Data, Catalog low baseline and applicable TxDOT security requirements.

- B) For Sensitive Data, Catalog low baseline with Sensitive overlay and applicable TxDOT security requirements.
 - C) For Confidential Data, Catalog moderate baseline and applicable TxDOT security requirements.
 - D) For Regulated Data, Catalog moderate baseline, applicable TxDOT security requirements, and applicable regulated security requirements.
- 2) TX-RAMP Requirements for Cloud Computing Services
- A) If TxDOT determines, in its sole discretion, and informs Vendor that the Work requires compliance with the requirements of DIR's Texas Risk and Authorization Management Program, Vendor (a) represents and warrants that it complies with the requirements of TX-RAMP Level 1 and Level 2, and (b) agrees that throughout the term of the Contract Term, it shall maintain its certifications and comply with the program requirements in the performance of the Contract.
 - 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 TxDOT.

4.6. Laws and Regulations

Vendor shall comply with all applicable federal and state laws and regulations related to the performance of the Work. A non-exhaustive list of federal and state laws and regulations that might be applicable includes the following:

- 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 Government Code, Chapter 2063 – Texas Cyber Command.
- G) Texas Penal Code, Chapter 33 – Computer Crimes.
- H) For Confidential Data, Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information.
- I) For Confidential Data containing Protected Health Information, Texas Health and Safety Code, Chapter 181 – Medical Records Privacy, and the federal Health Insurance Portability and Accountability Act (“HIPAA”), 45 CFR Part 160, 162 and 164.
- J) For Regulated Data containing Payment Card Industry (“PCI”) information, the Payment Card Industry Data Security Standards (“PCI-DSS”).
- K) For Regulated Data containing Criminal Justice Information (“CJI”), the Criminal Justice Information Services (“CJIS”) Security Policy.

4.7. Prohibited Technologies

In accordance with the Texas Statewide Plan for Prohibited Technologies, Vendor shall not provide services, equipment, or systems to TxDOT determined to be [Prohibited Technologies](#) by TxDOT.

4.8. Background Checks Required for Access to TxDOT Data and TxDOT Systems

- a) Vendor shall ensure that a background check is performed on each Vendor prior to that person receiving access (i) to any TxDOT System or (ii) in any Vendor Environment to TxDOT Data that requires a moderate or high-security baseline (as defined in the Catalog).
- b) 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 arrests 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.
- c) Vendor shall not allow any Vendor for which Vendor received any unfavorable result when conducting a background check to access TxDOT Data or any TxDOT System.
 - d) TxDOT may make exceptions to the requirements of this section on a case-by-case basis. Any exception granted by TxDOT must be in writing to be effective.
 - e) Upon request by TxDOT, Vendor shall provide documentation that demonstrates to TxDOT's satisfaction that background checks have been conducted as required and that no Vendor with one or more unfavorable results has received access to TxDOT Data or any TxDOT System.
 - f) Vendor shall immediately notify TxDOT if it learns of any change in status that might cause a Vendor to receive an unfavorable result from a background check.

4.9. Interconnection of TxDOT and Vendor Environment

If a Vendor has or will have one or more interconnections between an Information System in that Vendor's Environment and a TxDOT System or Systems, Vendor shall execute or cause to be executed an Interconnection Security Agreement ("ISA"), found on the [Cybersecurity Resources](#) page, for each interconnection. An executed ISA must be provided to TxDOT for each new interconnection prior to connection.

Upon request by TxDOT, Vendor shall provide any additional information or documentation that TxDOT determines is necessary to confirm a Vendor's compliance with this section.

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

4.10. SOC 1 Type 2 and SOC 2 Type 2 Requirements

If a Vendor is determined by TxDOT in its sole discretion 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 – Vendor must provide TxDOT the audit SSAE 18 Results within 15 days of Vendor's receipt of final report from independent auditor. Vendor will engage a third party 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").

4.11.

In addition, Vendor 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 TxDOT, Vendor must make available Vendor personnel to discuss with TxDOT the reports. Other report types will not be considered to meet these requirements.

4.12. TxDOT Virtual Desktop Infrastructure Requirements

If Vendor is provided with a user account to access TxDOT Virtual Desktop Infrastructure (TxDOT VDI), Vendor shall comply with the following TxDOT VDI requirements unless otherwise explicitly authorized in the Agreement:

- a) Data Residency. All TxDOT Data must remain solely on TxDOT systems located within the United States of America. Vendor will not store, process, or transmit TxDOT data outside the United States without express written approval from TxDOT.
- b) Remote Access Security. Any access to TxDOT VDI must be performed using Vendor-managed devices. Upon request, Vendor must provide written attestation that such devices meet TxDOT security requirements.
- c) Data Transfer Restriction. Vendor shall not transfer, copy, or move any TxDOT data from a TxDOT System to the Vendor’s environment without express written approval of TxDOT.

4.13. Health and Safety Code Compliance

- a) To the extent that this Contract involves the purchase or lease of computer equipment, Vendor certifies its compliance with Health and Safety Code Chapter 361, Subchapter Y and the Texas Commission on Environmental Quality rules in 30 TAC Chapter 328.
- b) To the extent that this Contract involves the purchase or lease of covered television equipment, Vendor certifies its compliance with

Health and Safety Code Chapter 361, Subchapter Z, related to the Television Equipment Recycling Program.

5. ARTIFICIAL INTELLIGENCE

5.1.

The use of AI functionality or AI Systems not described in the AI Explanation is not permitted without TxDOT's written consent.

5.2.

Vendor's AI program must include processes and controls sufficient to meet the requirements mandated under applicable AI Laws and TxDOT AI policy. Those measures will be set forth in a Vendor Artificial Intelligence policy, including all documentation needed to demonstrate compliance with AI Laws. Vendor will make that policy available to TxDOT upon request, along with descriptions of the controls in place for the AI technology, and will provide any other information requested by TxDOT regarding Vendor's responsible AI practices and policies.

5.3.

Vendor will, at its expense, implement and maintain appropriate technical and organizational measures to ensure any AI System used or developed in connection with or incorporated into the Work, and any Work intended to be used with or incorporated into an AI System, complies with AI Laws and TxDOT AI policy, including requirements related to the ethical or responsible use of Artificial Intelligence technology.

6. DEFINED TERMS

The following terms have the meanings set forth below solely for the purposes of this Attachment. To the extent a capitalized term is used but not defined in this Attachment, the term will have the meaning assigned to it in

the Contract. These definitions will not affect the interpretation of any other part of the Contract.

6.1. Affiliate

“Affiliate” means any legal entity that directly or indirectly owns, is owned by, or is commonly owned with Vendor. For purposes of this definition, to “own” means to have more than 50% ownership or the right to direct the management of the entity.

6.2. Artificial Intelligence

“Artificial Intelligence” or “AI” means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

6.3. Artificial Intelligence System

“Artificial Intelligence System” or “AI System” means any application that contains an AI component regardless of size or usage.

6.4. AI Laws

“AI Laws” means any laws applicable to Vendor or TxDOT relating to artificial intelligence systems and technology.

6.5. Baseline

“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 on the [Cybersecurity Resources](#) page.

6.6. Breach

“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.”

6.7. Cloud Computing Service

“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.

6.8. Confidential Data

“Confidential Data” includes each of the following categories of data:

- a) Any data that a Vendor accesses or downloads from a TxDOT System for use, manipulation, storage, or management unless otherwise specified in writing by TxDOT;
- b) Dates of birth of living persons;
- c) Driver’s license numbers;
- d) License plate numbers;
- e) Credit card numbers;
- f) Insurance policy numbers;
- g) Attorney-client communications;
- h) Drafts of policymaking documents;
- i) Information related to pending litigation;
- j) Audit working papers;
- k) Competitive bidding information before contract awarded;
- l) Personal Identifiable Information;
- m) Sensitive Personal Information;
- n) Regulated data;

- o) Information excepted from disclosure requirements of Chapter 552 of the Texas Government Code (“Texas Public Information Act”) or other applicable state or federal law;
- p) Compliance reports for which the Texas Attorney General has granted permission to withhold; or
- q) Investigative working papers and draft reports excepted from disclosure under Section 552.116 of the Texas Government Code.

6.9. Cybersecurity Incident

“Cybersecurity Incident” means any (a) unauthorized disclosure of or access to, loss, modification, disruption, or destruction of TxDOT Data, including Confidential Data; or (b) a weakness, flaw, or error found within Vendor’s systems that has a reasonable likelihood to be leveraged by a threat actor (i) related to Vendor’s handling of TxDOT Data or (ii) impacting TxDOT operations, network, or systems.

6.10. Environment

“Environment” means an aggregate of procedures, conditions, and objects affecting the development, operation, and maintenance of an Information System.

6.11. Human-in-the-Loop

“Human-in-the-Loop (HITL)” means a process in which a human decision-maker is actively involved in reviewing, validating or overriding the outputs of an AI System. In HITL systems, the AI System provides inputs, recommendations, or predictions that the human decision-maker evaluates and approves, modifies or rejects before any final decision or action is taken.

6.12. Information System

“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.

6.13. Personal Identifying Information

“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; or
- d) Unique electronic identification number, address, or routing code.

6.14. Public Data

“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.

6.15. Regulated Data

“Regulated Data” means information for which the use and protection of is dictated by a state or federal agency or by third party agreements.

6.16. Sensitive Data

“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.

6.17. Sensitive Personal Information

“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.

6.18. TxDOT Data

“TxDOT Data” means data, records, and information to which a Vendor has access or possession or which is otherwise provided by TxDOT, including data generated or collected under the Agreement, intellectual property developed under the Agreement, and Personal Identifying Information.

6.19. TxDOT Security Questionnaire

“TxDOT Security Questionnaire” means a cybersecurity and privacy questionnaire that provides TxDOT ITD necessary information for third party attestation in accordance with TxDOT requirements.

6.20. TxDOT System

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

6.21. Vendor

“Vendor” means Vendor, Subcontractors, or Affiliates (including any employees, agents and officers thereof).

6.22. Vendor Environment

“Vendor 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.