Policy Notice P-ITD-ISO-002

Policy Title: TxDOT Data Classification

Effective Date: Oct 16, 2024

Approved By: Marc D. Williams, P.E., Executive Director Marc D Williams box SIGN 4YWRZRR3-1RK2LY3W

Division of Primary Responsibility: **Information Technology**

Purpose

The TxDOT Data Classification policy establishes the framework for classifying TxDOT-owned data to ensure it is cost-effectively protected according to legal requirements throughout its lifecycle. At a high level, this policy addresses three factors to develop a risk-based approach for protecting TxDOT-owned data. The policy:

- Describes fundamental principles that define how TxDOT classifies data;
- Lists, clarifies, and provides examples of the data classification categories;
- Provides the roles and responsibilities for classifying data, securing data, and complying with the requirements of each category.

These factors address how TxDOT complies with the Texas Department of Information Resources (DIR) regulatory requirements, in accordance with Texas Administrative Code, defines data classification categories and ensures those who work with this data are aware of their responsibilities.

Delegation Authority

In accordance with TxDOT Policy Notice P-STR-001 Policy on Enterprise Policy, Feb. 20, 2022, TxDOT Executive Director delegates signature authority for this policy to the Chief Information Officer (CIO).

Scope

This policy is mandatory and applies to all data used to conduct TxDOT business, including what is received, created, collected, processed, used, shared, disseminated, maintained, or disposed. Individuals, including contractors and subcontractors, who use TxDOT-owned or TxDOT-held data must comply with this policy.

Policy

Data is an asset that must be protected from creation or receipt through its timely and authorized disposition. TxDOT owns the data created or used in support of its business activities, regardless of the form or format. TxDOT-owned or TxDOT-held data must be maintained in a secure, accurate, and reliable manner and must be readily available for authorized use.

The intent of this Data Classification policy is to define the data classification categories required by 1 TAC §202.24 and to provide the requirements Information Owners — individuals with the operational authority for the data — must use to classify TxDOT data. This assists in:

- Providing cost-effective protection for all TxDOT data while meeting legal requirements;
- Addressing ethical, privacy, and security concerns;
- Providing Information Owners security guidance;
- Ensuring data is protected in all states (at rest, in transit, and in use);
- Using disposal methods that provide the required protection of the classification assigned to the content.

TxDOT uses four categories to classify data: Public, Sensitive, Confidential, and Regulated. The Public category is the least restrictive. The Regulated category is the most restrictive. These categories apply to all TxDOT data regardless of format or age, whether digital or hard copy, newly created or scheduled for disposal. Data sent to the Texas State Library and Archives Commission for storage must be classified into one of these categories and remains TxDOT data.

Protection Requirements

Commingling Impact on Data Classification. When data from differing classifications are intermixed with each other, then all the data must be treated as if it were classified to be in the most restrictive category. Commingling data can occur when it is created, transmitted, used, stored, or disposed. Any kind of commingling of data commits TxDOT to the minimum level of protection of the *most restrictive category applicable to the commingled data.*

Default Classification. TxDOT data that has not been classified by the Information Owner must be treated as if it were in the Confidential category.

Disposal Requirements. Sensitive, Confidential, and Regulated data must be disposed in a manner that protects the data according to its classification category.

Data Owned by Third Party. TxDOT must protect all the data it uses that is owned by a third party to the degree specified in the Interconnection Security Agreement (ISA).

Exceptions. When TxDOT receives data from a third party that has not been classified, the TxDOT Information Owner receiving the data must classify the data according to the requirements of this policy.

TxDOT Information Owners *may* consider using additional protections beyond those specified in the ISA when their business judgment determines that the data's criticality to TxDOT's business processes warrants the additional protections.

Data Classification Definitions

TxDOT's data classification categories are derived from laws, regulations, and industry standards. They are approved and adopted by the agency's Executive Director and, in accordance with 1 TAC §202.24, compliance with them is monitored and reported through TxDOT's Information Security Program. TxDOT's Information Security Office notifies information owners, custodians, and users when business practices are noncompliant with the agency's information security policies, in accordance with 1 TAC §202.21(b)(12). TxDOT defines four classification categories listed below:

Public. Data that is considered Public has been defined in the Texas Public Information Act (PIA) as information that was "written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business" and which further meets the criteria specified in Texas Government Code §552.002. Information in the Public category is openly available and can be freely distributed by any TxDOT employee to anyone.

Examples include:

- Agency publications such as news releases or informational brochures;
- Public web postings, brochures, etc.;
- Description of TxDOT's Divisions or District organizations.

Sensitive. The Sensitive category is defined as data that is public information, releasable under the PIA, with restrictions that allow for its routine business use. Data in this category must be reviewed as part of TxDOT's Open Records Request process before it can be released. This restriction provides a safeguard through an established process. Some types of Sensitive data may be exempt from required release by the PIA. Coordinate with the General Counsel Division to determine if information classified as Sensitive is not subject to or if it is exempt from the PIA.

Examples include:

- Agency operational information, personnel records, internal communications, internal organizational charts, contact lists with business phone numbers, or business email addresses;
- Legal information, employment agreements, separation agreements, nondisclosure agreements, intellectual property, or contracts;
- Financial information about the agency's accounting such as balance sheets, purchase orders, contracts, or budget information.

Confidential. Data in this category must be protected from unauthorized disclosure or public release based on Texas law, federal law, or other legal agreements. This includes exemptions listed in the PIA, Protected Health Information that is protected by the Texas Medical Records Privacy Act, and all Sensitive Personal Information. Coordinate with the General Counsel Division to determine if such information is exempt from release.

Examples include:

- Information technology system vulnerability reports, architecture, and design;
- Incident investigations, including emails or conversations about them;
- Medical, legal, or financial information about a specific individual.

Regulated. Regulated data has its use and protection dictated by a federal agency or by third-party agreements and must meet the appropriate statutory definitions or industry agreement conditions.

Examples include:

- Bridge Special Inspection Reports. These are maintained per National Bridge Inspection Standards regulated by 23 USC §144 and §407.
- Payment Card Information. When credit card data is issued by American Express, Discover Financial Services, JCB International, Mastercard Worldwide, or Visa Inc then the Payment Card Industry (PCI) information is regulated by PCI Data Security Standards (DSS).
    - Payment card information regulated by PCI-DSS is Cardholder data: Primary Account Number (PAN), cardholder name, expiration date, and service code.
    - Sensitive Authentication Data: Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.
- Personal Information from State Motor Vehicle Records. Personal Information as defined in 18 U.S.C. 2725(3) means information that identifies an individual and obtained by TxDMV in connection with a motor vehicle record, except as provided in subsection (b) of the Driver's Privacy Protection Act is regulated by federal law (see Driver's Privacy Protection Act).

Roles and Responsibilities

The State of Texas assigns legal responsibilities for data classification to individuals in the following key roles: the Agency Head, the Information Security Officer, the Information Owner, the Information Custodian, Data Privacy Officer, and the Information User. These roles and their legal requirements are discussed here.

Agency Head. TxDOT's Executive Director reviews and approves all categories used to classify information except Confidential and Regulated categories which are dictated by law. The Executive Director or delegates issues the Data Classification policy and mandates its use.

Chief Information Officer. The CIO must:

- Review and issue changes to the Data Classification policy as needed;
- Administer its use throughout the Enterprise;

- Work with the Chief Information Security Officer (CISO), Information Owners, and Information Custodians to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.

Chief Information Security Officer. The CISO must establish procedures and practices necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.

Information Owner. Information Owners must assess how an accidental misuse or purposeful abuse of information affects their business unit's ability to support TxDOT's mission. Understanding the consequences of the loss of confidentiality, integrity, or availability informs the classification process.

Responsibilities. Information Owners must:

- Follow this policy to classify data;
- Classify the data under their authority;
- Coordinate with the CISO to assign security control requirements for data based on the classification category;
- Authorize Information Custodians to implement security control requirements and procedures to protect data;
- Remain accountable for exceptions to security control requirements.

Data Privacy Officer. The Data Privacy Officer reviews and validates that all classifications of Personally Identifiable Information (PII), Sensitive Personal Information, and Personal Health Information, are accurately assessed, classified, and marked.

Responsibilities. The Data Privacy Officer must provide guidance and assistance to senior agency officials, the CISO, Information Owners, Information Custodians, and Information Users about state or federal privacy laws and other applicable laws that may require public notification.

Information Custodian. When formally delegated by the Information Owner, the Information Custodian must:

- Implement controls required to protect information assets based on classification and risks specified by the Information Owner, this policy, TxDOT's Information Security Program, and the processes, procedures, standards, and guidelines that inform them.
- Provide information necessary for training employees with the appropriate information security needs.

Information Users. Individuals who work with TxDOT information must understand and comply with this Data Classification policy and must use the protection mechanisms and prohibitions prescribed under its authority to prevent intentional or accidental disclosure to unauthorized individuals and unintentional modification or destruction of TxDOT data. All TxDOT employees must formally acknowledge that they will comply with the security policies and procedures.

Order of Precedence

When there are conflicts between this TxDOT Data Classification policy and the provisions of the Texas Public Information Act or other local, state, federal law, or regulatory requirement, those provisions take precedence only where they are more restrictive than TxDOT requirements.

Definitions

Agency Head — TxDOT's Executive Director

Information Owner — A person(s) with statutory or operational authority for specified information or information resources

Information — Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [Source: 1 TAC §202.1].

Information Resources — The procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors [Source: Tex. Govt. Code §2054.003]

Information Resources Technologies — The data processing and telecommunications hardware, software, services, supplies, personnel, facility resources, maintenance, and training [Source: Tex. Govt. Code §2054.003]

Information Security Program — TxDOT's policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function [Source: 1 TAC §202.1].

Information System —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, sensors, communications, and people [Source: 1 TAC §202.1]

Integrity — The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. [Source: 1 TAC §202.1]

Network Security — The protection of computer systems and technology assets from unauthorized external intervention or improper use. The term includes detecting, identifying, and countering malicious network activity to prevent the acquisition of information or disruption of information technology operations. [Source: Tex. Govt. Code §2059.001]

Personal Identifying Information (PII) — Information that alone or in conjunction with other information identifies an individual, including an individual's name, Social Security number,

date of birth, government-issued identification number, mother's maiden name, unique biometric data, such as the individual's fingerprint, voice print, and retina or iris image. The definition also includes unique electronic identification number, address, or routing code. [Source: Tex. Bus. & Comm. Code §521.002]

Public Information — Information that is written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business. Public information is defined in the *Public Information Act*, Texas Government Code §552.002. Exemptions from release as public information are listed in Subchapter C, "Information Exempted from Required Disclosure." Other state laws also provide exemptions not listed in the Act.

Sensitive Personal Information — An individual's first name or first initial and last name in combination with any one or more of the following unencrypted items: social security number, driver's license number or government-issued identification number, account number, 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. Also, information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, payment for the provision of health care to the individual. However, the term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government [Source: Tex. Bus. & Comm. Code §521.002].

TxDOT Data — TxDOT Data is information that is written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business:

- by TxDOT;
- for TxDOT where TxDOT owns the information, has the right of access to the information, or spends or contributes public money for the purpose of writing, producing, collecting assembling, or maintaining the information; or
- by an officer or employee of TxDOT in the officer or employee's official capacity and pertains to official business of the government body.

This includes intellectual property, state records, and travel information.

See the following statutes for more information:

- Public Information in the Texas Public Information Act, Texas Government Code Sec. 552.002
- Intellectual Property as defined in 43 Texas Administrative Code §22.21(5)
- State records as defined in Texas Government Code Sec. 441.031
- Electronic records as defined in Chapter 5, Section 1 "Definition of an Electronic Record" of Records Management Manual
- Travel Information as defined in 43 TAC §23.2(7)

User of an information resource — An authorized TxDOT employee, contractor, partner, customer, guest, who has been granted privileges to access the agency's information

systems and its data. The user of an information resource may be another automated system.

For additional definitions of terms found in this policy, refer to TxDOT's Security and Privacy Glossary.

References

Tex. Govt. Code Ch. 552, Texas Public Information Act

Tex. Govt. Code §552.002. Definition of Public Information

Tex. Govt. Code Ch. 552, Subchapter C – Information Excepted from Required Disclosure

Tex. Govt. Code §2054.135. Data Use Agreement

Texas Business and Commerce Code §521.002. Unauthorized Use of Identifying Information

Texas Department of Information Resources. 2021. "Data Classification Template."

Office of the Attorney General of Texas. "Public Information Act Handbook."

Texas Department of Information Resources, Office of the Chief Information Security Officer. 2018. "Data Classification Guide." Identifying the goals, processes, and benefits of data classification.

PCI Security Standards Council. 2018. https://www.pcisecuritystandards.org/document_library/.

Texas Administrative Code, Title 1, Chapter 202
§202.1 — Applicable Terms and Technologies for Information Security Standards.
§202.21 — Responsibilities of the Information Security Officer.
§202.22 — Staff Responsibilities.
§202.24 --- Agency Information Security Program.

Texas Administrative Code, Title 43, Chapter 23. Travel Information

TxDOT. Records Management, 2022.

18 U.S.C. §2721: Prohibition on release and use of certain personal information from State motor vehicle records.

23 U.S.C. § 144: National bridge and tunnel inventory and inspection standards.

23 U.S.C. § 407: Discovery and admission as evidence of certain reports and surveys

US Department of Health and Human Services. 2017. "*National Institutes of Health." HIPAA Privacy Rule: Information for Researchers.* https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html December 18.

Version History

Version	Date	Updated By	Job Title / email address
2020.1	June 9, 2020	Cheryl Grant	Information Security Policy Coordinator / Cheryl.Grant@TxDOT.gov
2022.1	April 14, 2022	Kerry Pettit	Information Security Technical Writer / kpetti-c@TxDOT.gov
2023.1	Aug. 16, 2023	Cheryl Grant	Information Security Policy Coordinator / Cheryl.Grant@TxDOT.gov
2024.1	Sept. 6, 2024	Cheryl Grant	Information Security Policy Coordinator / Cheryl.Grant@TxDOT.gov

Brief Description of Change

2024.1 Scheduled review of policy. Added to the Sensitive category "The Sensitive category is defined as data that is public information" to make the definition explicit; removed responsibilities under Chief Information Security Officer now listed in the *Information Security and Privacy p*olicy to eliminate duplication; added Bridge Special Inspection Reports as an example under the Regulated category; and reformatted examples under each classification category for consistency.

Policy Owner

Steven Pryor, TxDOT Chief Information Security Officer, (ITD)
Steven.Pryor@txdot.gov (512) 965-4487