THE TEXAS STATE UNIVERSITY SYSTEM®

Data Management Policy

August 2025

Table of Contents

Texas State University System
Data Management Policy

Purpose

The Texas State University System (TSUS) acknowledges the significance of robust data management in safeguarding the confidentiality, integrity, and availability of its data and information assets. This policy, in accordance with Texas regulatory requirements, provides a framework for responsible and ethical data usage across the university system.

Scope

This policy applies to the TSUS and its member institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in their use of institutional data assets.

Application

The statements in this document establish the minimum requirements for TSUS each member institution. At the discretion of the member institution, more stringent, restrictive, or enhanced requirements may be established.

Management

This policy is managed by the TSUS Data Management Committee and TSUS Information Security Council and will be reviewed at least every five years, or more frequently as needed, by the chief data officer and appropriate member institution data management officers.

Policy/Procedure

1. Policy Statement

1.1. Each TSUS member institution is required to designate a full-time employee (or proxy) to serve as the Data Management Officer (DMO) in accordance with TGC §2054.137(b), establish a Data Governance Program as required by 1 TAC §218.20, and perform biennial data maturity assessments as mandated by TGC §2054.515(2). Each DMO, in conjunction with the TSUS Chief Data Officer and the institution's Information Security Officer (ISO), will support the TSUS and the institution's strategic operations and planning by defining, communicating, and leading the implementation of data governance and data management practices that comply with standards established under TAC §2054 and TGC §2063, while seeking and promoting cross-divisional data sharing opportunities to support cost savings and improve management outcomes.

2. Definitions

2.1. Data Asset: Any structured or unstructured data that has value to an institution. Data assets include student data, financial data, operational data, and any other data important to the institution. Data assets can be stored in databases, spreadsheets, or other formats and accessed through applications or analytics tools.

2.2. Data Architecture: How data are structured, integrated into business processes, and controlled for effective management by an organization.

2.3. Data Governance: The exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets.

2.4. Data Governance Program: A collection of structured approaches and activities to ensure data is reliable, confidential, accessible, and functional. These include policies, procedures, and standards that guide data collection, storage, management, and use. A data governance program supports data quality, data integration, data privacy, information security, and effective data architecture.

2.5. Data Management: The management of data asset creation, storage, access, and use.

2.6. Data Owner: An individual responsible for the oversight of an information resource or data asset.

2.7. Data Custodian: An individual or team charged by the data owner to provide information asset services to data owners and data users.

2.8. Data Steward: A data custodian responsible for planning, prescribing, and managing the sourcing, use, documentation, and maintenance of data assets. Functional data stewards are required to be knowledgeable regarding data assets in relation to business processes. Technical data stewards are expected to be knowledgeable about the underlying structure and administration of data assets. It is possible that a data steward could have both functional and technical knowledge.

2.9. Data Quality Management: Data quality management includes processes and procedures used to ensure data assets are free from errors and inaccuracies, as well as methods for change management and data cleansing.

2.10. Data Stakeholders: An individual or group who affects, or would be affected by, data policy or procedural change. A stakeholder requests data, initiates requests for changes to data that are impeding normal daily operations. They provide input or feedback that assists with the process of satisfying any change requested.

2.11. Other Relevant Technical Policy Terms: TSUS defines other relevant technical policy terms in the TSUS IT Policy information technology glossary.

3. Data Management Officer

3.1. Member institutions should ensure the DMO has the authority to accomplish key responsibilities outlined in TGC §2054.137 and TAC §218.20, as well as the ability to engage the institution's leadership as needed to ensure all stakeholders comply with the data governance program. The DMO should have data management expertise and is responsible for managing the institution's data assets and ensuring compliance with applicable laws and regulations. The DMO's key responsibilities include, but are not limited to:

3.1.1. Collaborating with the State's chief data officer, TSUS chief data officer, and the institution's ISO to ensure adherence to relevant rules and regulations.

3.1.2. Serving as a member of the State's Data Management Advisory Committee.

3.1.3. Participating in the TSUS Data Management Committee.

3.1.4. Establishing and maintaining a data governance program and related processes and procedures to identify and manage the institution's data assets in accordance with TGC §2054.137 and TAC §218.20.

3.1.5. Coordinating with the institution's ISO, Records Management Officer (RMO), and the Texas State Library and Archives Commission (TSLAC) to:

3.1.5.1. implement best practices for managing and securing data in accordance with state privacy laws, data privacy classifications, and cybersecurity standards established by the Texas Cyber Command under TGC §2063,

3.1.5.2. ensure the institution's records management programs apply to all data storage media, and

3.1.5.3. conduct a data maturity assessment of the institution's data governance program in accordance with the requirements established by TAC §218.

3.1.6. Developing and facilitating employee data management and literacy training programs.

3.1.7. Ensuring at least three high-value data sets, as defined by TAC §2054.1265, are posted to the Texas Open Data Portal.

4. Data Governance Program

4.1. The Data Governance Program shall provide the framework for effective data management, ensuring transparency, auditability, stewardship, and accountability. At a minimum, the program must:

4.1.1. Catalog, classify, and label data assets, as well as assign ownership and accountability for these assets to ensure effective stewardship.

4.1.2. Promote data quality through widely accepted data and reporting standards, definitions, documentation, and best practices.

4.1.3. Provide efficient and effective access to data while complying with institution policies related to information security and data privacy.

4.1.4. Communicate data quality and reporting initiatives across the institution.

4.1.5. Empower data owners to develop and enforce policies and procedures for consistent data management and reporting.

4.1.6. Ensure compliance with relevant state and federal laws related to data management, including cybersecurity requirements established by the Texas Cyber Command under TGC §2063.

5. Data Maturity Assessment

5.1. As required by TGC §2054.137(3)(D), TGC §2054.515(2), and TAC §218, each institution's designated DMO, with assistance from the institution's designated ISO, shall conduct a data maturity assessment at least once every two years.

5.2. The data maturity assessment will include at least the following elements:

5.2.1. Data Architecture

5.2.2. Data Analytics

5.2.3. Data Governance and Standardization

5.2.4. Data Management and Methodology

5.2.5. Data Program Management and Change Control

5.2.6. Data Quality

5.2.7. Data Security and Privacy

5.2.8. Data Strategy and Roadmap

5.2.9. Master Data Management

5.2.10. Metadata Management

5.3. Institutions shall complete their data maturity assessment using the Texas Department of Information Resources' (DIR) Data Management and Analytics Maturity Assessment (DMAMA) tool or an equivalent assessment tool that meets the requirements of TAC §218.20 and aligns with cybersecurity standards established by the Texas Cyber Command.

6. Data Classification

6.1. Each institution shall establish a data classification framework which, at minimum, includes all requirements specified in the TSUS IT Policy (Risk Assessment Policy §4.2.2, Security Planning Policy §4.1.4, Security Planning Policy §6, and Assessment, Authorization, and Monitoring Policy §5.1.2.4).

6.2. All institutional data shall be labeled according to its classification level to enable appropriate handling, protection, and compliance with TSUS IT Policies and Texas Business and Commerce Code §521.002.

7. Data Sharing

7.1. Each institution's DMO and ISO shall collaboratively develop standard data sharing agreements in compliance with Texas Government Code §2054.0286 (the statewide data program) for the secure exchange of data with external entities.

7.2. When sharing sensitive or confidential data within the TSUS or between state agencies, institutions shall use the standard TSUS inter agency data sharing agreement, which includes the elements prescribed in the Texas Statewide Data Exchange Compact (TSDEC) established by DIR.

7.3. All data sharing activities must comply with relevant state and federal privacy laws including, but not limited to, FERPA (20 U.S.C. § 1232g) for student records and HIPAA (45 CFR Parts 160 and 164) for health information where applicable.

8. References

8.1. Texas Government Code Title 10, Subtitle B, Chapter 2054 – Information Resources, Section 2054.137 and 2054.515

8.2. Texas Government Code Title 10, Subtitle B, Chapter 2063

8.3. Texas Administrative Code Title 1, Part 10, Chapter 218, Subchapter C, Section 218.20

8.4. Texas Business and Commerce Code Section 521.002

8.5. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g

8.6. Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160 and 164

8.7. The Texas State University System Information Technology (IT) Policy

8.8. Texas Administrative Code Title 1, Part 10, Chapter 202 (TAC §202) - Information Security Standards

8.9. Texas State Library and Archives Commission (TSLAC)