TEXAS TECH UNIVERSITY

Operating Policy and Procedure

OP 73.01: Data Management and Data Governance

DATE: July 7, 2023

PURPOSE: The purpose of this Operating Policy/Procedure (OP) is to establish an enterprise-wide policy and procedures for data management and data governance at Texas Tech University.

REVIEW: This OP will be reviewed in January of odd-numbered years by the Data Stewardship Council and Data Governance Board with substantive revisions forwarded to the President.

POLICY/PROCEDURE

1. Introduction

Pursuant to Texas Government Code, Chapter 2054, Section 137, Texas Tech University is required to designate a Data Management Officer and establish a Data Governance Program.

a. Data Management Officer

The Data Management Officer is required to coordinate with the State Chief Data Officer to ensure that Texas Tech University performs assigned duties, such as improving the control and security of information and promoting the sharing of information between state agencies. Additional duties include developing best practices, including interagency information coordination; reducing duplicative information collection; increasing accountability; ensuring compliance with rules requiring agencies to share information; improving information management and analysis to increase security; uncovering fraud and waste; reducing agency costs; improving operations; and verifying compliance with applicable laws.

b. Data Governance Program

The Data Governance Program responsibilities include the following:

(1) Identify data assets, exercise authority and management over data assets, and establish related processes and procedures to oversee agency's data assets.

(2) Coordinate with agency's information security officer to:

(a) Implement better practices for managing and securing data in accordance with state privacy laws and data privacy classifications;

(b) Ensure agency's records management programs apply to all types of data storage media;

(c) Increase awareness of and outreach for agency's records management programs; and

(d) Conduct a data maturity assessment of the agency's data governance program in accordance with the requirements established by department rules.

(3) Data Classification, Security, and Retention Requirements – On initiation of an information resources technology project, include an application development project and any information resources projects described.

(4) Coordinate the Agency Information Security Assessment and Report every two years.

(5) Submit the Data Maturity Assessment in June of each year to the Texas Department of Information Resources. The Data Maturity Assessment provides information and assessment of continued improvement in each of the following categories:

(a) Data Architecture
(b) Data Analytics
(c) Data Governance and Standardization
(d) Data Management and Methodology
(e) Data Program Management and Change Control
(f) Data Quality
(g) Data Security and Privacy
(h) Data Strategy and Roadmap
(i) Master Data Management
(j) Metadata Management
(k) Open Data Portal

2. Data Governance

Texas Tech University has a Data Governance Program that includes a Data Governance Board and Data Stewardship Council. Data Governance facilitates the development of a data-centric organization that values data through all phases of its lifecycle and ensures data quality that demonstrates the ability to make decisions based on insights from analytics. The primary business drivers for Data Governance are to reduce risk, including data security and privacy, and to improve processes related to compliance, data quality, metadata management, data project efficiencies, and vendor management.

a. Data Governance Board

The Senior Vice President for Administration & Finance and Chief Financial Officer will chair the Data Governance Board with the Chief Data Management Officer as the co-chair. The Data Governance Board will include all Texas Tech University vice presidents who are also Data Owners including the Chief Information Officer (CIO) and Vice President for Information Technology, Vice President for Enrollment Management, Vice President for Research & Innovation, and Provost and Senior Vice President. The Data Governance Board will act as a steering committee, meet quarterly, and provide strategic direction and oversight for the Data Stewardship Council. The Data Governance Board will also sponsor projects through the Data Stewardship Council that improve data quality, improve productivity, increase efficiency, or address compliance issues.

b. Data Stewardship Council

The Chief Data Management Officer will chair the Data Stewardship Council. Members will include nominees from each of the Data Governance Board members and will meet monthly. The Data Stewardship Council will also include rotating members known as Stewardship Project teams who are directly involved with or impacted by projects. In addition, Response Team Members will be included to support specific project requirements. The Data Stewardship Council will provide project updates, recommendations, and other information back to the Data Governance Board.

The Data Stewardship Council and Stewardship Project teams will focus on creating and managing core metadata, documenting rules and standards, managing data quality issues, and executing operational Data Governance activities.

3. Applicability

This policy applies to all employees of TTU that are involved with data project decisions, Data Owners, Data Stewards, or employees involved at any level of data management.

4. Data Asset Inventory and Classification

a. Procedure

The TTU Data Owner is responsible for data classification. Per TTU OP 52.01, Information Technology (IT) Operations, "All institutional data that is classified as Confidential, Sensitive, Regulated, Mission-Critical, or is otherwise subject to restricted access requirements, must be stored or processed only on information resources located in the University Data Center."

TTU Data Owners will be responsible for submitting and classifying all Data Assets to the Chief Data Management Officer for all existing and new assets. Outputs that are generated from data assets that are used for external and/or official reporting will also include outputs and reporting cycle schedules.

b. Compliance

Departments will be required to conduct an annual review to ensure that the Data Asset Inventory is accurate, correctly classified, and outputs are accurate.

5. Data Project Management

a. Procedure

The TTU Office of the CIO has an IT Project Registration application. With coordination through the Office of the CIO and oversight of the Data Governance Board and Data Stewardship Council, a subset of projects meeting the definition of data project will be submitted to the Chief Data Management Officer to ensure projects meet Texas Tech University requirements, are relevant, and do not create a duplication of effort.

b. Compliance

Submission of the data project to the Data Governance Board is required. It is incumbent upon the department to demonstrate that projects are effectively managed, and metrics are in place to track progress.

6. Data Quality

a. Procedure

The Office of the Chief Data Management Officer will conduct an annual Data Quality Assessment for systems of record, sensitive/regulated data, or systems used for external reporting.

Data Quality Assessments will evaluate:

- Accuracy
- Completeness
- Consistency
- Integrity
- Reasonability
- Timeliness
- Uniqueness/Deduplication
- Validity

b. Compliance

Department Data Owners, Data Stewards, and Technical Staff, where they exist, that oversee a system of record, sensitive/regulated data, or systems used for external reporting are required to actively participate in the assessment and the development of a post assessment action plan. The post assessment action plan will support continuous improvement and be evaluated on subsequent assessments.

A critical element of Data Quality is the Business Glossary, and departments will be required to have up-to-date and clear definitions for mission critical data for which Data Owners and Data Stewards will be held accountable.

Business Glossaries that apply to the general campus will be published and available in the Data Governance SharePoint site to support accessibility, search capabilities, and access to documented institutional knowledge. Published Business Glossaries will not include information related to security or information that may be considered sensitive. Detailed technical models will fall outside the scope of the Business Glossary requirements, but departments are encouraged to maintain technical models to support ongoing operations. The Office of the Chief Data Management Officer and Data Stewardship Council is available to provide recommendations for developing technical models or business glossaries.

c. Business Glossary Components and Function

(1) Definitions of Key Terms;

(a) Reference Data that falls under a "Key Data Element" classification should be explicitly identified in the document.

(2) Enables a common understanding of the core business concepts and terminology;

(3) Reduces the risk the data will be misused due to inconsistent understanding of business concepts;

(4) Defines internal processes and procedures related to quality control, data lineage, and data auditability;

(5) Improves alignment between technology assets and business organizations;

(6) Terms and definitions must be associated with metadata; and

(7) Links to external references related to business rules or compliance.

7. Key Data Element Changes

a. Procedure

Departments are required to demonstrate appropriate controls over who is authorized to make programmatic changes or database updates to Key Data Elements. Key Data Elements will be identified and maintained through the Data Asset Inventory.

b. Compliance

Designated Data Owners or Data Stewards are required to communicate any programmatic additions, updates, or removal of Key Data Elements to the Chief Data Management Officer. The Chief Data Management Officer will route changes through the Data Stewardship Council and Data Governance Board to ensure that all potential downstream impacts are accounted for, specifically for changes that may impact official reporting or compliance.

c. Key Data Elements

(1) Also referred to as a Critical Data Element;

(2) Defined by an external agency and is used in multiple internal/external reports;

(3) Is related to regulatory compliance;

(4) Material impact on business operations;

(5) Used to derive or calculate another element that is flagged as a Key Data Element;

(6) Impacts other elements; and

(7) Quality will impact model and analytical calculations.

8. Resolving Data Issues

a. Procedure

Resolving data issues is a core function of Data Governance and can directly or indirectly impact multiple Data Management areas including efficiency, data quality, and compliance. The Data Governance Board and Data Stewardship Council provide an orderly and predictable escalation path for resolving issues.

b. Compliance

Data Issues should be submitted to afdmd.staff@ttu.edu.

9. Records Management

a. Procedure

The Chief Data Management Officer will coordinate with the Chief Information Security Officer and Records Management Officer to ensure that departments have implemented records management processes that adhere to their data domain's retention requirements and that data is secure in accordance with state privacy laws and data privacy classifications for all data storage media.

b. Compliance

Departments are required to follow OP 10.10, Records Retention, implement a records management protocol for their specific data domain, and demonstrate that required processes are followed. The Data Stewardship Council can provide assistance with the development of records management protocol.

10. Definitions

a. Data Governance Roles

(1) System Administrator – Technical experts who have been given the authority to make changes to database architecture or related interfaces. Systems Administrators are also responsible for security, data storage, and operations.

(2) Data Owner – Accountable for the data within a specific domain and has authority to approve changes. Data Owners are responsible for:

(a) Approving data glossaries and data definitions;

(b) Ensuring the accuracy of information;

(c) Directing data quality activities;

(d) Reviewing and approving master data management approaches, outcomes, and activities;

(e) Working with other data owners to resolve data issues; and

(f) Providing second-level review for issues identified by Data Stewards.

(g) Can serve on the Data Stewardship Council.

(3) Data Steward – Accountable for the day-to-day management of data and are subject matter experts (SMEs) who understand the meaning and use of the information they manage. Data Stewards are responsible for:

(a) Being SMEs for their data domain;

(b) Identifying data issues and working with other data stewards to resolve them;

(c) Reporting to the data owner and other stakeholders within a data domain; and

(d) Working cross-functionally across lines of business to ensure their domain's data is managed and understood.

(e) Can serve on the Data Stewardship Council.

(4) Response Team Members – Data Stewardship Council project team members formed to complete projects or resolve issues. May include team members outside of the Data Stewardship Council.

b. Data Classification Levels

(1) Public – Information that is freely and without reservation made available to the public.

(2) Sensitive – Information that could be subject to release under an open records request but should be controlled to protect third parties.

(3) Confidential – Information that typically is excepted from the Public Information Act.

(4) Regulated – Information that is controlled by a federal regulation or other third-party agreement.

Attachment A: Data Accountability Metrics for Texas Tech University