STANDARD ADMINISTRATIVE PROCEDURE

29.01.01.M0.01 University Data Governance and Management

Approved December 4, 2024
Next scheduled review: December 4, 2029

Standard Administrative Procedure Statement

Texas A&M University endeavors to utilize all institutional data generated at Texas A&M University to drive meaningful insights, foster innovation, and empower decision-making at every level of our organization that will derive ongoing value from this data utilization.

We envision a future where institutional data is a strategic asset that, at the foundation, is incorporated into University strategic goals and students' success, to transform the way we serve, interact, and engage our students, employees, community, and citizens of the state of Texas by moving Texas A&M data utilization from descriptive analytics to predictive and prescriptive analytics.

Reason for Standard Administrative Procedure

Data Management is the development, execution and supervision of plans, programs, and practices that deliver, control, protect, and enhance the value of data and information assets throughout the Data Life Cycle. This SAP will address the data, processes or controls that are not governed by TAMU SAP 15.99.03.M1.03, *Responsible Stewardship of Research Data* and TAMU SAP 29.01.03.M0.01, *Security of Electronic Information Resources*.

Definitions

Refer to Texas A&M Information Security Controls Catalog
https://it.tamu.edu/policy/it-policy/controls-catalog/index.php

Institutional Data - Data related to the operation and functioning of the university and the institution's educational mission.

Procedures and Responsibilities

1. GENERAL

    1.1. Governing law and jurisdiction

1.1.1. Texas SB475 87th Session enacted governance for a Data Management Officer for state institutions with more than 150 full-time employees. This position is charged at each institution for establishing data ethics, principles, goals, strategies, standards, and architecture. This position also coordinates with the Chief Information Security Officer and Chief Records Management Officer to bridge the gap between the business and technology enterprises of the University.

1.1.2. The Chief Data Management Officer continuously assesses the institution's data maturity and inform the appropriate Vice Presidents of recommendations to move the maturity progress forward. The Chief Data Management Officer utilizes the data maturity tool as prescribed on the State of Texas DIR site, Digital Maturity Assessment Tool. The Chief Data Management Officer will also hold the title of Data Management Officer as outlined in 1.1.1.

1.1.3. According to Section 2054.070 three high-value data sets as defined by Section 2054.1265 must be posted on the Texas Open Data Portal. The Chief Data Management Officer strategizes and consults with the Provost, Vice Presidents or equivalent to identify these high-value data sets, such as degrees conferred, number of students enrolled, average class sizes, etc.

1.1.4. TAMU follows the Data Management Associations DAMA (DAMA) International Data management Body of Knowledge or DAMA-DMBOK as the standard for all data programs and processes and the abbreviated Fast Start Learning Guide or FSL.

1.1.5. TAMU shall establish a Federated Data Operating Model. This data operating model provides a centralized strategy with decentralized execution. Federation enables the organization to prioritize based on specific data entities, divisional challenges, or unit priorities. The University Data Governance Committee will review requests submitted from the IT Data Governance Committee and will make decisions, to shape and continuously stay current with the dynamic environment of data, as they align with strategic priorities and initiatives set by University leadership.

1.2. Data Principles

1.2.1. Data is an institutional asset with unique properties. Unlike other assets, data is not consumed when used. Data is used to inform decisions that affect students, faculty, staff, and the citizens of Texas. Data has an economic value, and it is imperative to determine how that value can be accessed and by whom.

1.2.2. Data must be secure.

1.2.3. Data must be accurate and of the appropriate quality as established by the University that determine data is 'Fit for Purpose'. Data standards must be established in order to ensure data possesses the following six core measured dimensions: completeness, uniqueness, timeliness, validity, accuracy and consistency.

a. Completeness. The degree to which all requisite information is included and data values have no missing elements.

b. Uniqueness. No data point will be recorded more than once based upon how that (data point) is identified.

c. Timeliness. The degree to which the currency of data aligns with business needs.

d. Validity. Data is valid when conforms to the established definition of format, type, range, etc.

e. Accuracy. The degree to which data correctly describes the event being analyzed.

f. Consistency The absence of difference when comparing two or more representations against the defined definition time after time.

g. Data quality should focus on the data most critical as defined by University Administration through the Strategic Plan.

h. Standardizations for data, including institutional name changes etc. shall be determined by the University Data Governance Committee with implementation by the IT Data Governance Committee.

1.2.4. Data must be available in a single aggregation of data sources and accessible to those who have been authorized through existing data access request processes.

1.2.5. Minimum standards and expectations of data literacy for data stewards, data custodians, data managers and data users must be established and implemented to ensure data is utilized ethically and appropriately and is constantly evolving to keep up with the change. (Refer to roles listed in 2.2)

2. DATA MANAGEMENT ROLES

2.1. Data Governance Executive Committee & Roles

a. Chief Information Officer
b. Chief Technology Officer
c. Chief Data Management Officer
d. Provost and Executive Vice President or designee
e. Vice President of Planning, Assessment & Strategy or designee

2.2. Data Stewards - describes an individual with a role title related to representing information—for a specific information type, business sector, or business function—for university-wide information governance purposes. An example of a Data Steward in the student data domain is the University Registrar; an example in the financial/budget data domain is the Chief Financial Officer. Data Stewards are institutional officers and have management and policy-making authority over their specific data subject areas, including the business definitions of data, and the access and use of that data across the university.

2.2.1. Ensure that information systems that store or process university *data* remain compliant with university security controls and all applicable federal and state regulations.

2.2.2. Remediate or mitigate risks related to *data* under their care identified through the annual information security risk assessment process.

2.2.3. Appoint *Data Managers* for their *data* subject areas.

2.3. Data Managers - are responsible for the quality and integrity of a defined dataset on a day-to-day basis. Data Managers evaluate and authorize requests for access to the *data*, and ensure data is protected from misuse or mismanagement. Data Managers are assigned these responsibilities by a *Data Steward* over a particular data domain and may act as a delegate of the Data Steward for routine purposes. An example of a Data Manager in the student data domain is the manager of a college advising office.

2.3.1. Establish procedures to protect the quality and integrity of assigned datasets that align with the Data Governance Executive Committee vision and strategies.

2.3.2. Evaluate and authorize (or deny) requests for access to assigned datasets and review access on a regularly established timeline.

2.3.3. Delegate authority to Data Custodians as appropriate for *data* administration.

2.4. Data Custodians - are information technology professionals who manage the information systems that store and process university *data*. Data Custodians develop and implement technology infrastructure to support the functional needs of a data domain, and implement technical security controls to ensure the confidentiality, integrity, and availability of data under their care.

2.4.1. Assist Data Stewards in classifying university *data* and information resources according to the university data classification standards as outlined in Texas A&M Information Security Controls Catalog-Data Classification.

2.4.2. Implement security controls required by the Texas A&M Information Security Controls Catalog.

2.4.3. Follow system monitoring procedures described in Audit and Accountability.

2.4.4. Follow incident reporting guidelines as described in Incident Response.

2.4.5. Ensure university *data* is recoverable in accordance with risk management decisions.

2.5. Data User - refers to any individual (student, employee, or affiliate of the university) who interacts with university *data*.

2.5.1. Data Users must adhere to TAMU SAP 29.01.03.M0.02, *Information Resources - Acceptable Use.*

2.6. Any type of Data not specifically mentioned in this SAP, must adhere to existing procedures, e.g. research and student data.

2.6.1. The use of these data for purposes outside of operational and educational purposes (e.g., research) will be evaluated by the University Data Governance Committee

3. ACCESS AND USE

3.1. Data is classified according to the IT Policy Data Classification Policy & Procedures (DC-1) and Access follows the described process in each detailed classification category with the exception of Automatic Access outlined in 3.2.1.

3.1.1. Data is categorized into the following categories:

- Public

- University-Internal
- Confidential
- Critical

3.1.2. Automatic Access to data shall be granted to the University offices that are responsible for the mandatory state, federal, and accreditation reporting entities upon approval by the AVP or VP of the respective employee requesting access. All required trainings will be applied to the user as outlined according to the Data Steward's access policies.

3.1.3. Access Review: When a Data Steward or Data Manager deems that access to the requested data does not meet Texas A&M University expectations for business need, the University Data Governance Committee can hear an appeal for the request when presented up through the appropriate Dean or Vice President to the committee.

3.2. Institutional data shall not be used for machine learning models unless clear goals and outcomes have been defined and in accordance with applicable TAMUS policies and regulations.

4. UNIVERSITY DATA GOVERNANCE COMMITTEE COMPOSITION

This committee is responsible for delivering decisions to the Data Governance Executive Committee on all University topics related to institutional data. Research data and decisions are managed by the Vice President of Research.

4.1. The University Data Governance Committee will provide the IT Data Governance Committee the overarching goals and strategies for the committee to then deploy into operations and develop appropriate monitoring and adherence checks.

4.2. The University Data Governance Committee is composed of top-level executives, assistant dean equivalent or higher, within the organization that is knowledgeable of Texas A&M's overall operations and be able to speak on behalf of a division and/or unit specifically on data related topics, processes, adherence and/or use of. Representation will be sought from the following areas and the Data Governance Executive Committee can expand inclusion beyond this.

a. Chief Data Officer
b. Chief Information Officer
c. Chief Technology Officer
d. Faculty Senate Representative
e. University Staff Council Representative
f. Council of Deans Representative
g. Department Head Steering Committee Representative
h. Representative of Vice President for Planning, Assessment & Strategy
i. Representative of Student Affairs
j. Representative of Vice President of Finance & Business Services
k. Representative of Vice President Human Resources & Organizational Effectiveness
l. Representative of Provost and Executive Vice President's Office
m. Representative of the Associate Vice President for Enrollment Management's Office

n. Representative of the Associate Vice President for Academic Effectiveness and Planning
o. Representative of the Office of Ethics, Risk, and Compliance.

4.3. Decisions in committee meetings will be made when quorum of ten (10) members are present to vote.

4.3.1. The Data Governance Executive Committee is responsible for confirming or overturning decisions made by University Data Governance Committee.

Related Policies or Requirements or Statutes

Texas Govt. Code Title 10, Sect. 2054.0332
Texas Data Management Framework Fast Start Learning Guide
DAMA-Data Management Body of Knowledge 2nd Edition
System Policy 29.01, *Information Resources*
System Regulation 29.01.01, *Information Resources Governance*
University SAP 13.02.99.M0.01, *Student Records*
University SAP 15.99.03.M1.03, *The Responsible Stewardship of Research Data*
University SAP 17.02.02.M0.02, *Technology Mediated Materials and Instruction*
University SAP 17.02.02.M1.01, *Procedures for Technology Mediated Instructional Material*
University SAP 29.01.03.M0.01, *Security of Electronic Information Resources*
University SAP 29.01.03.M0.02, *Information Resources - Acceptable Use*
University Rule 29.01.99.M1, *Information Resources*
Texas A&M Information Security Controls Catalog

Contact

Vice President for Planning Assessment and Strategy