LAMAR UNIVERSITY
DATA GOVERNANCE POLICIES

SECTION: Data Governance
AREA: Institutional Data

Number: xx.xx.xx

SUBJECT: Data Governance Policy Program

I. PURPOSE AND BACKGROUND

Lamar University is a committed steward of its institutional data, providing a framework to ensure the security, privacy, integrity, quality, and governed usage of produced data throughout the data life cycle.

Institutional data are a critical component of Lamar University's operations and decision-making process. Without proper governance, the University may engage in inefficient practices or be exposed to undue risk.

In response to Texas Senate Bill 475, the University has designated a Data Management Officer, formed a Data Governance Committee, initiated an internal review of all data systems and practices, and designed and instituted a set of data governance policies.

The Data Governance Committee was formed in Fall 2022 and is comprised of a robust cross-section of campus leaders. After the formation of working groups conceptually focused on policy, definitions, and data systems, a general data governance framework was developed. The framework focuses on quality processes by which people interact with data, the systems and technology facilitating and delivering data to stakeholders, the security of the data systems, the privacy of its users, and the overarching governance guiding the University in its data usage. The designed framework and subsequent data governance policies were endorsed and adopted by the committee and executive leadership for use across the University. The policies allow for greater fidelity of implementation for practices involving data systems and processes.

II. SCOPE

This policy applies to all faculty, staff, and students who leverage data systems and data produced by these systems on behalf of Lamar University.

III. CORE PRINCIPLES AND FRAMEWORK

The data governance policy is constructed along four core principles (Figure 1):

A. A hierarchy of data governance and ownership.
B. Processes that define data quality and the associated data certification processes.
C. Established data security and privacy policies.
D. A well-defined range of data definitions that span multiple systems and functional areas across the University.

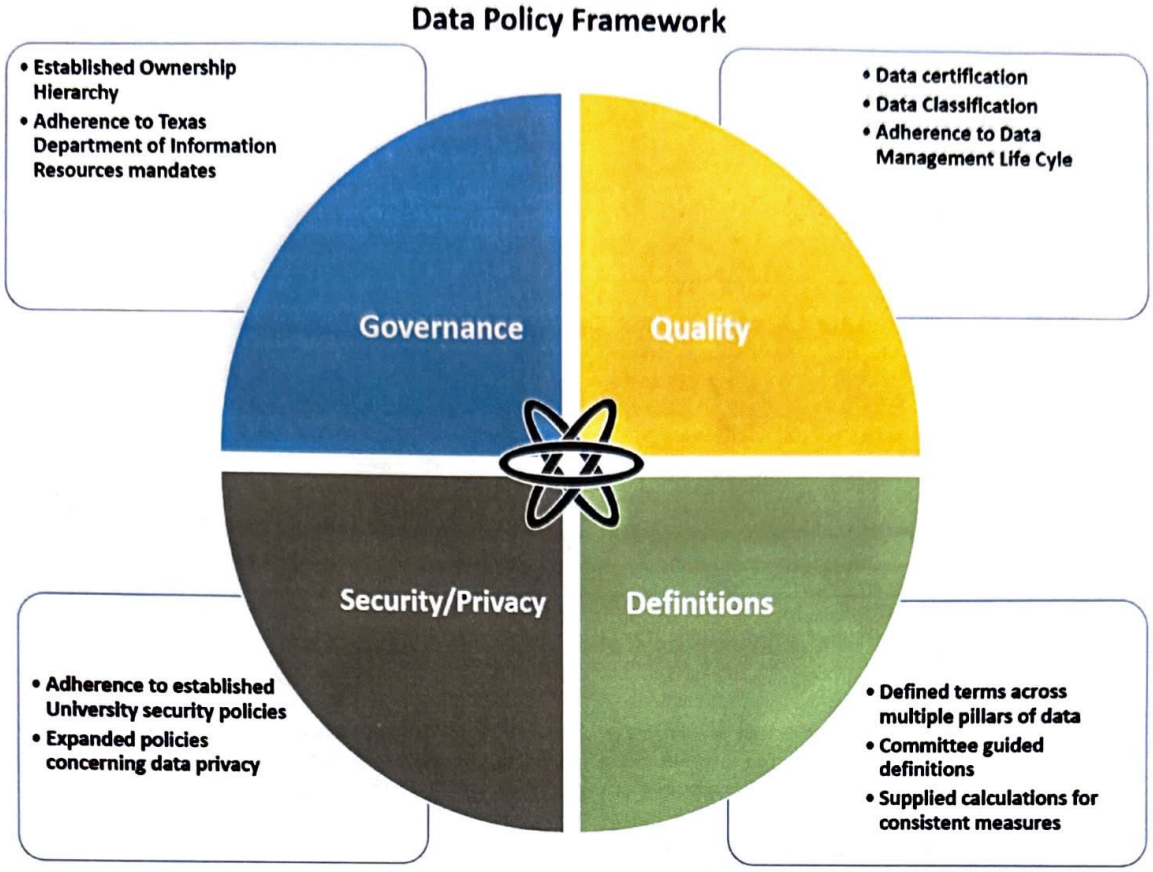

Figure 1.

A. STRUCTURE OF DATA GOVERNANCE AND OWNERSHIP HIERARCHY

1. Executive
   1.1. Data Executives
      1.1.1. Examples of key Data Executives include the University President, Provost, and Chief Financial Officer (CFO).
      1.1.2. Act as the ultimate authority and responsible party for the institution's data.
      1.1.3. Provide approval for policies and guidelines generated by the Data Governance Committee.

2. Guidance and Strategy
   2.1. Data Management Officer
      2.1.1. Establishes and maintains data governance program.
      2.1.2. Classifies data.
      2.1.3. Facilitates the Data Governance Committee.
      2.1.4. Posts high-value data sets to the Texas Open Data Portal.
   2.2. Data Governance Committee
      2.2.1. Determines data governance policies and guidelines for executive approval.
      2.2.2. Defines key terms to build a consensus language around data across the University.
      2.2.3. Catalogues and monitors University data systems to determine compliance, ownership, and need.

3. Stewardship
   3.1. Data Owner
      3.1.1. Acts as primary point of contact for their requisite system.
      3.1.2. Charged with overseeing data quality.
      3.1.3. Provides guidance for update parameters.
      3.1.4. Sets permissions for data access (covers ad hoc requests as well as larger system-level integrations).
   3.2. Data Stewards
      3.2.1. Act on behalf and, at times, under direction of the Data Owner.
      3.2.2. Serve as subject matter experts for their requisite system.
      3.2.3. Are responsible for day-to-day activities and maintaining the guidelines set by the Data Owner.
      3.2.4. Serve as a resource for Functional personnel.

4. Functional
   4.1. Data Specialists
      4.1.1. Report on data systems and support Data Consumers and Producers.
      4.1.2. May update data systems under direction of Data Owner.
      4.1.3. Work with Data Owners to resolve errors.
      4.1.4. Direct access to data systems.
      4.1.5. Serve as technical subject matter experts.
   4.2. Data Consumers
      4.2.1. Leverage data governance framework to guide usage.
      4.2.2. Provide feedback to Stewardship personnel as to data quality, format, and need.
   4.3. Data Producers
      4.3.1. Follow procedures defined by Stewardship personnel to load data in the proper format and context.
      4.3.2. Perform data corrections prescribed by Stewardship personnel.

5. Ancillary or External
   5.1. Vendors
      5.1.1. Provide data-related services.
   5.2. Auditors
      5.2.1. Conduct investigations into data systems and processes to determine fidelity of data and reporting.

B. DATA QUALITY AND CERTIFICATION PROCESSES

Data Producers and Consumers are expected to follow appropriate procedures when inputting and consuming system data. There is also an expectation that system data will be current, and any discovered inconsistencies or errors will be resolved in a timely manner to facilitate high data fidelity. Data Stewards, in conjunction with Data Specialists, should work to verify and vet outputs for quality, consistency, and integrity. All University data should adhere to the adopted Data Management Life Cycle (Figure 2).

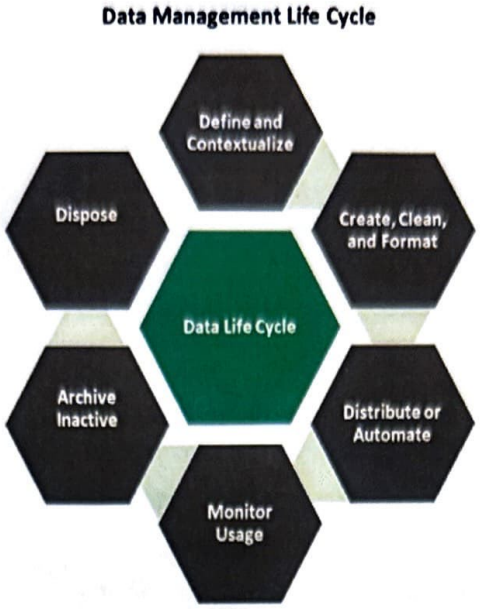

Figure 2.

1. Define and Contextualize
   1.1. Data should be certified and classified using the Data Certification and Data Classification levels contained in the University's Data Governance Policy.

2. Create, Clean, and Format
   2.1. Data reports may be created across a variety of systems but should adhere to the same general practice throughout development. Data Specialists will work in conjunction with Data Owners and Data Stewards to create data reports. Data checks will occur between Data Specialists and Data Owners and Data Stewards. Data Specialists will also include Data Consumers during the formatting process.

3. Distribute or Automate
   3.1. Data outputs (reports, files, etc.) should be scheduled or distributed via the appropriate platform utilizing the correct security controls in place.

4. Archive Inactive
   4.1. When archiving or inactivating data, the existing University policies on records management should be followed.

5. Dispose
   5.1. When disposing of University data, the existing University policies on records management should be followed.

Data and reporting platforms will adhere to a system of certification and classification that informs users as to the supplied data's requisite status concerning the fidelity of the data being supplied and the determined limits upon uses and capacity for distribution.

1. Data Certification

1.1. Certified for Official Reporting

1.1.1. In general, these data will adhere to methodology provided by either the Texas Higher Education Coordinating Board (THECB) or the Integrated Postsecondary Education Data System (IPEDS) or other state or federal regulatory body. Data have been cleaned, vetted, and used for official University reporting.

1.2. Certified for Internal Reporting

1.2.1. In most instances, these will be live data from the Banner ERP system that are dynamic and subject to daily change. Known data issues have been documented and common data definitions can be found in the Data Glossary. Data are intended to be used for internal decision-making.

1.3. In Progress

1.3.1. Data reports that are under active development and, as such, although the initial form and layout of associated reports are in place, they are not final. Some data definitions may not be available in the Data Glossary. All issues may not be known or fully documented.

1.4. Not Certified

1.4.1. No quality checks have been applied. Associated reports are at the earliest stage of development. All risks are fully assumed by the user.

2. Data Classification

2.1. Restricted (Red)

2.1.1. The highest level of security is required. Mishandled Restricted data could result in criminal or civil penalties. Access is granted on a case-by-case basis by the Data Owner. Advanced security protocols are enforced for both the storage and transmission of this Data Classification.

2.2. Confidential (Orange)

2.2.1. Although not as tightly controlled as Restricted data, strict access control is still required for the Confidential level. Access is typically granted on a per job basis or via system access roles. Security protocols are expected to be followed for the storage and transmission of this Data Classification.

2.3. Internal (Yellow)

2.3.1. Data accessible by employees for general University business. Care should still be taken in the storage and transmission of this Data Classification.

2.4. Public (Green)

2.4.1. While there can be some restriction placed on this Data Classification, the data are still generally releasable to the public online or through an open records request.

C. DATA SECURITY AND PRIVACY

Data governance will generally follow guidelines established by existing University IT security policies. At a minimum, those interacting with University data should:

- Maintain the confidentiality and integrity of University data.
- Adhere to and maintain compliance with applicable laws, codes, controls, rules, and regulations.
- Adhere to data certification and classification protocols.
- Adhere to all established University IT security policies in any interaction with University data.

With respect to student data privacy involving education records, the University complies with the privacy standards established by the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and other applicable federal and state laws.

Both students and employees have the option to request a hold on any publicly available directory information that may be supplied via an open records request via the Public Information Act (PIA).

D. IDENTIFIED AND DEFINED TERMS

The University will maintain a glossary of identified and defined terms as related to University data and data governance. The complete glossary is housed on the public-facing website and will undergo a biannual review (December and May of each academic year) to revise existing terms as well as add new ones. The Data Management Officer is responsible for maintenance of the glossary and will facilitate updates through the Data Governance Committee.

V. ENFORCEMENT

Failure to adhere to the provisions of this policy statement may result in:

1. Loss of Lamar University Information Resources access privileges.
2. Disciplinary action up to and including termination for employees, contractors, or consultants.
3. Dismissal for interns and volunteers.
4. Suspension or expulsion in the case of a student.
5. Civil or criminal prosecution.

IV. REVISION AND RESPONSIBILITY

Oversight Responsibility: Office of Data, Analytics, Reporting, and Analysis

Review Schedule: Every two years

Last Review Date:

Next Review Date:

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	xx/xx/xxxx	xxx ....

V. APPROVAL

Chief Information Officer — Date of Approval: 2-14-24

President, Lamar University — Date of Approval: 2/15/24