LP 2.6

Effective:
5/5/2026

Revised:

Policy Owner:
Board of Trustees

Policy Administrator:
AVP Planning, Analytics & Decision-support; Chief Information and Technology Officer

Affected Parties:
Employees

Table of Contents:

Institutional Data Governance

1 Summary

Lander University recognizes that its data and information are critical institutional assets. The university is dedicated to implementing governance programs that promote responsible usage, ensure data availability for informed decision-making and operational support, and proactively manage risks. These governance programs are designed, developed, and sustained to serve the interests of the university and its diverse stakeholders. This policy sets forth the framework and responsibilities for governance of university data and information.

2 Purpose

This policy is designed to:

2.1 Establish and maintain a university-wide structure for governing data as a critical institutional asset.

2.2 Establish and maintain a unified approach for managing university data to ensure that data is accurate, consistent, accessible, interoperable, secure, and responsibly used.

2.3 Ensure that university data is collected, managed, accessed, and used to support operations and decision-making.

2.4 Assign clear responsibilities for data management across all units and data governance roles.

3 Scope

3.1 All university divisions, organizational units, and individuals share responsibility for upholding these standards and for managing data in compliance with applicable policies, regulations, and institutional expectations.

3.2 This policy is not binding upon content produced for or by teaching and learning activities, or upon academic research data that may be generated or maintained through activities, outputs, and findings of university faculty, students, and staff (see Intellectual Property policy LP3.2). However, with appropriate adaptation, the principles and framework of data governance presented in this policy may be extensible and beneficial to academic research data.

3.3 This policy operates in coordination with the University Information Security Program, Privacy Policy, and Information Security Standards.

4 Guiding Principles

The life cycle of data management will be guided by the following principles:

4.1 **Data Governance Framework**: To create a formal framework that includes a governance committee, policies, procedures, roles and responsibilities, data management tools, and training.

4.2 **Data Access and Compliance:** To promote appropriate data practices and compliance with relevant laws and regulations. Educate staff, students, and stakeholders about the approved use of data and the consequences of non-compliance.

4.3 **Data Quality and Integrity:** To implement processes and standards to maintain data accuracy, consistency, and reliability. Regularly assess and audit data to minimize errors and inconsistencies.

4.4 **Commitment to Transparency:** To foster a culture of transparency in data governance practices. Communicate data policies, procedures, and decisions openly to stakeholders, promoting trust and accountability.

4.5 **Utilizing a Single Source of Record:** To ensure that a single, authoritative source of data is defined for critical data elements. This "single source of record" should be maintained and regularly updated to eliminate data inconsistencies and duplication.

4.6 **Data Access and Authorization**: To define access controls and authorization processes to restrict data access to authorized personnel only. Implement role-based access control and enforce the principle of least privilege.

4.7 **Balance Governance with Operational Efficiency**: To support data governance processes that create institutional efficiency and timely operations and will be implemented in a manner that minimizes unnecessary administrative burden.

5 Definitions

5.1 **Access:** Authorization to view or use a given resource or asset (e.g., data, an information system).

5.2 **Artificial intelligence (AI):** Technology that increasingly enables computers and machines to simulate human learning, comprehension, problem-solving, decision-making, creativity, and autonomy. Applications and devices equipped with AI often include, but are not limited to, the capabilities of being able to see and identify objects, to understand and respond to human language, to learn from new information and experience, to make detailed recommendations to users, and to sometimes act independently, potentially replacing or reducing the need for human intervention.

5.3 **Constituents:** Persons and entities that have a relationship to any organizational unit of the university system, including, but not limited to students, employees, and other affiliates (e.g., board members, consultants, contractors, donors).

5.4 **Data and Information:** Refers to the individual or collective values, content, media (including audio, visual, and multimedia), intellectual property, official reports, and work products that the university and its units collect, process, transmit, store, or maintain. This encompasses all details about university constituents, business processes, events, operations, and services. In the context of AI, data also include inputs used to train AI models and algorithms, which transform raw data into meaningful insights, predictions, and decision-making tools. These AI-driven processes enable the university to enhance its operations while ensuring the responsible and ethical handling of data in compliance with applicable laws and regulations.

5.4.1 **Usage of "data":** Within this policy, "data" denotes institutional information assets as a whole and is treated as a collective (mass) noun, so singular verbs are used (e.g., "data is protected," "data is a critical institutional asset"). This convention is adopted for readability in governance and administrative contexts and does not restrict the use of "data" as a plural noun in research or methodological publications.

5.5 **Data Classification:** Descriptions of parameters of a data element reflecting risk, sensitivity (including whether the data element contains personal identifying information [PII]), data type, and what controls and measures must be applied to protect it from unauthorized access and use. Data classification also applies to assets, including storage hardware and systems, media, transmission or presentation, information systems, databases, and other data assets. If multiple data elements with different classifications are present in a file or repository, whether individually or combined, the classification of the file or repository is equivalent to the highest classification of any data element present. The university adheres to the State of South Carolina data classification schema:

5.5.1 **Public Information**: Information intended or required for sharing with the public.

5.5.2 **Internal Use**: Non-sensitive information that is used in daily operations of the university.

5.5.3 **Confidential**: Sensitive information used by the university, including PII.

5.5.4 **Restricted**: Highly sensitive information used by the university that is protected by statutory penalties if disclosed in an unauthorized manner, including PII.

5.6 **Data Consumer (Data End-User):** Refers to any person or system that accesses university assets, including data and information systems. Data users are responsible for using data only for authorized purposes, completing required training, reporting suspected breaches, and complying with applicable laws and regulations.

5.7 **Data Custodians:** Personnel who maintain hardware, information systems/ databases, applications, backup systems, and networks through which data is transmitted, processed, and stored. Custodians may be university personnel or personnel/service providers under agreement or contract with the university.

5.8 **Data Element:** Denotes a discrete and purposeful, often single, point of information; also known as a field, column, variable, or object.

5.9 **Data Standards:** Conventions, rules, and services adopted to ensure appropriate, consistent, and interoperable use of data and information across the university. Data Standards include agreed-upon definitions for data elements, metadata structures, data formats, data dictionary entries, naming conventions, coding schemes, and integration protocols. Data Standards are established and maintained by Data Stewards within their respective domains and are coordinated across domains by the Data Governance Steering Committee.

5.10 **Enterprise Information System:** Denotes a system-wide university resource that exists to manage essential administrative functions and transactions. A primary example includes, but is not limited to, Banner (a student information system).

5.11 **Information System:** Denotes a database, file, application, filing system, or other system that is used for a limited business function and is not necessarily available on all system campuses or to all departments on a single campus. Primary examples include, but are not limited to, Ellucian Banner, SLATE, StarRez, and Watermark.

5.12 **Permissions**: Describe what activities a data user is enabled to perform with the access they have been authorized for and granted, often based on job duties or functions; also known as user rights.

5.13 **Personal Identifying Information (PII)**: Data elements that are used as identifiers for persons and which, if compromised, may present a significant risk of identity theft or identity fraud. Under South Carolina Code of Laws, Section 16-13-510 (D), PII includes a person's Social Security number, driver's license number or state identification number, banking account numbers, date of birth, digital signatures, and current and former names and addresses, among other personal information items.

5.14 **Research Data:** Data generated, collected, observed, or derived through activities, outputs, and findings of university faculty, students, and staff in the pursuit of scholarly inquiry, creative works, or sponsored projects, including, but not limited to, experimental results, survey responses, observational records, computational outputs, and associated documentation and metadata. Research Data is subject to applicable federal and sponsor requirements (including NIH and NSF data management and sharing policies), as well as Lander University's Intellectual Property policy (LP3.2). While this policy does not govern Research Data directly, its governance principles and framework may be applied to Research Data with appropriate adaptation

5.15 **University Data**: Information deemed critical to the mission and operation of the university. Such data is often managed and distributed or exchanged across multiple organizational units within and beyond the university. An item may be a university datum if it meets one or more of the following criteria:

5.15.1 At least two organizational units use the data and consider them essential;

5.15.2 Integration of information systems requires the data;

5.15.3 The university must ensure the integrity, privacy, and security of the data to comply with legal, regulatory, competitive, or external reporting requirements;

5.15.4 A broad cross section of users refer to or maintain the data;

5.15.5 The university needs the data to plan, manage, audit, or improve its operations;

5.15.6 Unauthorized access to or use of the data represents an unacceptable risk to the university or its constituents, including data protected by the Family Educational Rights and Privacy Act (FERPA).

5.15.7 This definition excludes other information that may be a public record, personal property, intellectual property, academic research data, or content directly related to or produced through teaching and learning activities.

6 Data Governance Ownership

6.1 Lander University reserves the rights to all data, content, and information that it collects, generates, transmits, and stores relating to its constituents, services, programs, and operations.

6.2 All university divisions, organizational units, and individuals share responsibility for upholding these standards and for managing data in compliance with applicable policies, regulations, and institutional expectations.

6.3 The Data Governance Steering Committee must coordinate and collaborate with stakeholders of university data and information systems to implement, administer, and continuously improve data and information governance.

6.4 Project teams must engage with ITS early in the planning, design, implementation, and upgrading of information systems so that data governance actions (e.g., required data definitions, standards, and data sharing agreements) can be assessed and implemented.

7 Data Governance Roles and Responsibilities

7.1 Data Governance Steering Committee

The Data Governance Steering Committee ensures that data initiatives remain aligned with institutional priorities, that issues are addressed at the appropriate level, and that cross-domain challenges are resolved consistently and effectively. The committee:

7.1.1 Oversight

Ensures alignment of data initiatives with the university's mission, strategic plan, and long-term initiatives. Guide the data governance program to maintain consistent standards, practices, and accountability across the institution.

7.1.2 Training

Facilitates annual training opportunities for data stewards.

7.1.3 Resolution and Recommendation

Serves as the primary body for reviewing and resolving escalated data issues, with most matters expected to be addressed at the steering committee level. Only issues requiring executive judgment are elevated to data trustees for final determination.

7.1.4 Membership

Is composed of director-level (or higher) representatives from the following data domains and functional areas:

- Students
- HR/Employees
- Finance
- Administration
- Planning and Decision-Support
- Institutional Research
- Information Technology

7.2 Data Stewards

Data stewards are accountable for the quality, protection, and appropriate use of the data within the organizational unit they lead. They ensure that data is managed consistently, responsibly, and in alignment with institutional policies and operational needs. Under normal circumstances, data stewards make operational decisions about data in their care within the scope of established university policies, standards, and executive direction. Their core responsibilities include:

7.2.1 Establishing and maintaining division-level data governance guidelines and data standards

Defining and documenting standards for data elements within their domain, including the creation and upkeep of metadata and definitions used in the data dictionary that support clarity, consistency, and shared understanding across the university.

7.2.2 Documenting and communicating data governance policy data standards

Developing, maintaining, and communicating the rules, requirements, and regulatory obligations governing data in their domain. Data stewards ensure that data producers, users, and any affected units understand and follow these expectations.

7.2.3 Ensuring data quality and resolving data issues

Monitoring data for accuracy, completeness, and consistency and coordinating the resolution of data-related issues that affect their domain. This includes identifying root causes, implementing corrective actions, and collaborating with data producers and system owners to implement these corrective actions.

7.2.4 Participating in projects involving their data domain

Engaging in planning, design, and implementation activities for projects, systems, or processes that create, modify, or rely on data within their domain. Data stewards

ensure that new initiatives align with established standards and governance practices.

7.2.5 Managing and authorizing data access

Overseeing access to data within their domain by reviewing requests, determining appropriate levels of access, and ensuring that permissions align with security, privacy, and operational requirements. They ensure that access decisions are documented and compliant with university policy.

7.2.6 Promoting responsible data use

Supporting appropriate and ethical use of data by advising units and users, identifying risks, and ensuring that data-handling practices align with institutional expectations and legal requirements.

7.2.7 Collaborating across governance structures

Working with other data stewards, data trustees, data custodians, and university governance bodies to support consistent data practices, resolve cross-domain issues, and advance institutional data governance goals.

7.3 Data Trustee

Data Trustees provide executive-level oversight of the data domains under their authority. They ensure that data governance practices are embedded within institutional operations and that data is managed in alignment with the university's strategic priorities. Their responsibilities include:

7.3.1 Designating and overseeing Data Stewards

Identifying and appointing qualified individuals to serve as data stewards for each functional organizational unit, ensuring that stewardship responsibilities are clearly assigned and effectively carried out.

7.3.2 Promoting and championing data governance practices

Advocating for consistent, responsible data management across the university by supporting governance initiatives.

7.3.3 Setting strategic direction for data policy and priorities

Making high-level decisions regarding data-related policies, priorities, and resource needs. Data Trustees ensure that data governance aligns with institutional goals, regulatory requirements, and operational needs.

7.3.4 Offering executive guidance and resolving escalations

Acting as the final authority for issues needing executive decisions and providing definitive resolutions, when required.

7.3.5 Ensuring accountability within their organizational units

Confirming that units managing or using data within their domain adhere to data governance requirements, maintain data quality, and support secure and appropriate data use.

8 Escalation Path for Data Governance Issues

8.1 Data governance issues should be resolved at the lowest appropriate level. Most concerns related to data quality, access, compliance, or use are addressed by the data steward for the relevant organizational unit, who has primary responsibility for operational decisions.

8.2 Issues that cannot be resolved at the data steward level, or that present broader domain-level risk or impact, are escalated to the Data Governance Steering Committee.

8.3 When an issue cannot be resolved by the Data Governance Steering Committee or requires an executive judgment, it is escalated to the Data Trustees, who serve as the final decision authority and ensure that decisions align with the university's mission, strategic priorities, and risk tolerance.

9 Compliance and Enforcement

9.1 Data Trustees are responsible for ensuring adherence to the institutional data governance policy.

9.2 The Data Governance Steering Committee, through recommendations from data trustees and appointed data stewards, evaluates, updates, and/or upholds data policies and procedures in alignment with this policy.

9.3 Data consumers who violate this policy may have their access to university data suspended, either temporarily or permanently. Cases will be referred to the Data Governance Steering Committee, and disciplinary actions will follow university procedures with proper notice, documentation, and review.

9.4 Violations may result in termination of data access, reports to institutional authorities, and employment-related and/or legal consequences.

10 Policy Revision History

- First draft of policy created by Data Governance Co-chair on 2/16/2026.
- Revised by Policy Coordinator on 4/6/2026.
- Stakeholder review and provisional approval of policy on 4/13/2025.
- Final revisions applied by Policy Coordinator on 4/17/2026.
- Reviewed with comments by the Board of Trustees Policy Committee on 4/26/2026.
- Reviewed and revised by Data Governance Steering Committee on 4/292026.
- Approved by the Lander University Board of Trustees on 5/5/2026.