LP 7.9

Effective:
8/6/2026

Revised:

Policy Owner:
Board of Trustees

Policy Administrator:
Chief Information and Technology Officer

Affected Parties:
Faculty, staff, students

Table of Contents:

Policy Name

1 Purpose

1.1 Lander University relies on information and information technology systems to support its academic, administrative, and operational missions. University data and systems are institutional assets that require protection.

1.2 Lander University is committed to safeguarding the confidentiality, integrity, and availability of information in all formats and to complying with applicable federal and state laws governing privacy and data protection.

1.3 This policy establishes requirements for data privacy, data classification, and data protection.

2 Scope

2.1 This policy applies to:

2.1.1 All university colleges, departments, administrative units, and affiliated organizations.

2.1.2 All faculty, staff, students, contractors, affiliates, and authorized users of Lander University systems or data.

2.2 This policy is intended to complement, but not to replace, requirements under laws and regulations, including the Federal Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and research compliance and other applicable policies.

3 Definitions

University Data: Any information collected, created, received, maintained, or used by the university to conduct institutional business, regardless of format or storage medium.

4 Roles and Responsibilities

Protection of university data is a shared responsibility.

4.1 University data owners, data custodians, and departments responsible for data must:

4.1.1 Ensure that data is appropriately classified.

4.1.2 Implement measures and controls consistent with this policy.

4.1.3 Monitor compliance within their functional area.

4.2 System administrators and Information Technology Services (ITS) must:

4.2.1 Establish information security standards, procedures, and technical safeguards.

4.2.2 Provide guidance for secure storage of, transmission of, and access to data.

4.2.3 Review and approve technology solutions handling institutional and sensitive data.

4.3 Authorized users

4.3.1 All users must:

4.3.1.1 Access data only for legitimate university purposes.

4.3.1.2 Protect information according to its classification.

4.3.1.3 Report suspected misuse or security incidents.

4.3.2 Violations may result in disciplinary action, termination of data access, and/or legal consequences.

5 Data Privacy

The university respects the privacy of its students, employees, and partners, and of affiliated individuals.

The university must:

5.1 Use sensitive information only to support its institutional missions and legal obligations.

5.2 Limit data access to individuals with a legitimate business need.

5.3 Require data confidentiality obligations for employees and third-party partners.

5.4 Maintain agreements governing protection of institutional data.

6 Data Classification

Lander University data must be classified according to risk and legal requirements, using the following categories (please reference *Appendix A: Data Classification Schema and Guidelines*):

6.1 Public

6.1.1 Public data includes, but is not limited to, data intended for public dissemination (e.g., website content, brochures, press releases, published policies).

6.1.2 Unauthorized disclosure of public data presents minimal risk.

6.2 Internal use

6.2.1 Internal data includes, but is not limited to, nonpublic operational information that does not include regulated personal data (e.g., internal memos, draft agendas, training materials, aggregated data, agency procedures, and/or operating standards).

6.2.2 Unauthorized exposure of internal use presents limited institutional risk.

6.3 Confidential

6.3.1 Confidential data includes, but is not limited to, biometric identifiers, photographs of individual people, pension and retirement benefit information, security plans, and unpublished information about agency personnel.

6.3.2 Confidential data is protected by policy or contractual obligation where disclosure could cause institutional or individual harm.

6.4 Restricted

6.4.1 Restricted data includes, but not limited to, student education records, HR records, financial records, Social Security numbers, driver license numbers, protected health information, and other regulated or sensitive information.

6.4.2 Restricted data is highly sensitive information protected by law or regulation. Unauthorized disclosure may result in significant harm or statutory penalties.

6.5 Data containing multiple classifications must inherit the highest classification level. Information must be labeled and handled according to its classification.

7 Data Protection Requirements

7.1 Lander University must implement administrative, technical, and physical safeguards appropriate to data classification, including:

7.1.1 Controlled access based on a legitimate business need.

7.1.2 Encryption of confidential and restricted data during storage and transmission.

7.1.3 Secure handling of mobile devices, removable media, and cloud services.

7.1.4 Contractual protection when sharing data with third parties.

7.1.5 Secure disposal and media sanitization practices.

7.1.6 Protection of facilities housing critical systems and sensitive information.

7.2 Specific security standards and operational procedures must be maintained separately by ITS.

8 Data Access and Use

8.1 Access to confidential or restricted data requires authorization and accountability.

8.2 Disclosure of sensitive data is prohibited unless authorized or legally required.

8.3 Social Security numbers must not be used as identifiers or credentials.

8.4 Approved institutional systems must be used for storage and processing of Lander University data.

9 Third-Party and Cloud Services

Before sharing confidential or restricted data with external entities:

9.1 Appropriate contractual agreements must be implemented in alignment with Lander University policies and state and federal regulations.

9.2 Security responsibilities must be defined in alignment with Lander University policies and state and federal regulations.

9.3 ITS and Procurement approval is required where applicable.

10 Compliance and Enforcement

Failure to comply with this policy may result in:

10.1 Revocation of system access.

10.2 Disciplinary action.

10.3 Termination of employment or affiliation.

10.4 Civil or criminal penalties where applicable.

11 Supporting Procedures and Standards

11.1 Detailed security procedures, standards, and implementation requirements must be maintained and administered by ITS.

12 Related Policies

- Student Handbook
- Institutional Data Governance (LP2.6)
- Student Data Privacy and Protection (LP7.2)
- Research misconduct and human subjects research policies
- Human Resources policies governing staff conduct and performance
- Email Use for Faculty and Staff (LP7.1)
- Technology Acceptable Use (LP7.5)
- Website Privacy (LP7.6)

13 Policy Revision History

- First draft of policy created by Chief Information Technology Officer on 8/6/2026.
- Final revisions applied by Policy Coordinator on 8/7/2026.
- Reviewed by Board of Trustees Policy Committee on 8/11/2026.
- Approved by the Lander University Board of Trustees on 9/1/2026.

Appendix A: Data Classification Schema and Guidelines

Adapted from the State of South Carolina Enterprise Privacy Office[1]

Restricted	Confidential	Internal Use	Public Information
• Federal tax information received from, or derived from, the IRS or secondary sources (IRS Pub. 1075) • Protected Health Information (HIPAA/HITECH) • Individual financial information subject to GLBA • Social Security numbers • Debit or credit card numbers • Driver's license information or State identification card information • Bank account numbers or information with personal identification numbers (PINs) or passwords • Passport numbers • Child welfare and legal information about minors (juvenile justice, foster care and/or adoption) • Witness protection information • DNA record & profile contained in the State DNA database • Dates of birth (if linked to other information about a person) • Student education records • Trade secrets • Employee Identification Number	• Biometric identifiers • Photographs of individual people • Pension/Retirement benefit information (actual amounts) Personal demographics (race, place of birth, weight, religion) • Unpublished information about agency personnel • All information exempt from disclosure pursuant to §30-4-40 of the SC Code of Laws (SC Freedom of Information Act) • Information received from and/or about a business (tax information, business plans) • Security plans, network architecture, etc. • Passwords	• Agency policies, procedures, and/or standards • Training materials • Internal meeting information • Direct telephone line numbers to staff • Aggregated data	• Public-facing website content • Publicly distributed information • Meeting agendas and minutes from public meetings • Brochures • Press releases • Agency contact information

[1] South Carolina Department of Administration, Enterprise Privacy Office, Data Classification Schema and Guidelines, Version 2.0 (July 15, 2015), https://www.admin.sc.gov/sites/admin/files/Documents/PMOOTIS/Data_Classification_Schema_and_Guideline.pdf (accessed August 13, 2026).