LP 7.2

Effective:
4/29/2026

Revised:
5/11/2026

Policy Owner:
Board of Trustees

Policy Administrator:
Chief Information and Technology Officer; Registrar

Affected Parties:
Any individual with authorized access to student information

Table of Contents:

Student Data Privacy and Protection

1 Introduction

1.1 Lander University (the "university") is committed to protecting the privacy, confidentiality, integrity, and availability of student education records and related data. This policy establishes requirements for the collection, access, use, disclosure, storage, transmission, and protection of student information in accordance with applicable federal and state laws, institutional policies, and industry best practices.

1.2 This policy applies to all university faculty, staff, students, contractors, volunteers, third-party service providers, and any individual or system with authorized access to student information, regardless of format (electronic, paper, or verbal).

2 Privacy and FERPA Compliance

2.1 Lander University complies with the Family Educational Rights and Privacy Act of 1974 (FERPA), which governs access to and disclosure of student education records.

2.2 More information related to student rights, directory information, and FERPA protections can be found on the university's website at:

https://www.lander.edu/academics/registrars-office/ferpa.html

3 Information Security and Regulatory Alignment

3.1 Lander University safeguards student information in compliance with:

3.1.1 The Family Educational Rights and Privacy Act (FERPA)

3.1.2 The Gramm-Leach-Bliley Act (GLBA)

3.1.3 Applicable State of South Carolina information security and privacy requirements

3.1.4 University information security, data classification, and acceptable-use policies

3.2 As a participant in federal financial aid programs, the university maintains a comprehensive, risk-based information security program appropriate to its size, complexity, and data environment.

4 Security Objectives

The objectives of the university's Student Information Security Program are to:

4.1 Protect the confidentiality, integrity, and availability of student information.

4.2 Safeguard against anticipated threats or hazards, including cyber threats, unauthorized access, and data loss.

4.3 Prevent unauthorized use or disclosure of student information that could result in harm, identity theft, or loss of trust.

4.4 Ensure accountability and compliance with this policy across faculty, staff, and third-party partners.

5 Governance, Roles, and Responsibilities

5.1 Chief Information Officer (CIO): Oversight of information security strategy and policy alignment.

5.2 Designated IT personnel: Operational responsibility for security controls, incident response, risk management, and security awareness.

5.3 Registrar: Custodian of educational records.

5.4 Data and System Owners: Ensure appropriate access controls, accuracy, and security of systems managing student information in alignment with the Institutional Data Governance Policy (LP2.6).

5.5 All Users: Responsible for protecting student data and complying with policy and training requirements.

6 Information Security Safeguards

Lander University employs administrative, technical, and physical safeguards, including but not limited to the following.

6.1 Administrative Safeguards

6.1.1 Mandatory security and privacy training for all university faculty and staff, including annual refreshers.

6.1.2 The use of confidentiality and acceptable-use acknowledgments prior to system access.

6.1.3 Formal access provisioning and de-provisioning procedures.

6.1.4 Vendor due-diligence and contractual data-protection requirements.

6.2 Technical Safeguards

6.2.1 Role-based access control (RBAC) and least-privilege enforcement.

6.2.2 Secure authentication using university-managed credentials (e.g., SSO, MFA where required).

6.2.3 Encryption of student data in transit and at rest, as appropriate.

6.2.4 Centralized logging, monitoring, and intrusion detection.

6.2.5 Automated session timeouts for systems containing student information.

6.2.6 Removal of Social Security numbers from primary identifiers and use of institution-assigned ID numbers.

6.3 Physical Safeguards

6.3.1 Secure office layouts and privacy screens where student data is visible.

6.3.2 Controlled access to records storage areas.

6.3.3 Secure disposal of paper records via cross-cut shredding or certified destruction.

6.3.4 Secure media sanitization and destruction for retired hardware.

7 Incident Reporting and Response

Any suspected or confirmed compromise of student information must be reported immediately to the chief information officer (CIO).

The university maintains an incident response process that includes:

7.1 Incident identification and containment

7.2 Assessment of scope and impact

7.3 Coordination with designated stakeholders

7.4 Required reporting to state or federal authorities, when applicable

7.5 Notification to affected individuals when legally required

7.6 Post-incident remediation and review

8 Continuous Improvement

Student information security and privacy at Lander University is an ongoing process. This policy is subject to regular review and updating to reflect:

8.1 Changes in technology and instructional delivery methods

8.2 Emerging cybersecurity threats

8.3 Updates to laws, regulations, and state requirements

8.4 Institutional risk assessments and audit findings

9 Related Policies

- Institutional Data Governance (LP2.6) [1]
- Family Educational Rights and Privacy Act (FERPA) [2]
- Email Use for Faculty and Staff (LP7.1) [3]

---

[1] Institutional Data Governance policy URL: https://www.lander.edu/about/_files/documents/policies/lp-2_6-institutional-data-governance.pdf

[2] FERPA web page: https://www.lander.edu/academics/registrars-office/ferpa.html

[3] Email Use for Faculty and Staff policy URL: https://www.lander.edu/about/_files/documents/policies/LP-7_1-Email-Use-for-Faculty-and-Staff-b.pdf

- Technology Acceptable Use (LP7.5) [4]
- Website Privacy (LP7.6) [5]
- Vulnerability Management (LP7.7) [6]

10 Policy Revision History

- Initial draft prepared by Chief Information and Technology Officer in coordination with university Registrar on 4/29/2026.
- Prepared for review and provisional publication by Policy Coordinator on 8/10/2026.
- Approved by the Lander University Board of Trustees on 9/1/2026.

[4] Technology Acceptable Use policy URL: https://www.lander.edu/about/_files/documents/policies/LP-7_5-Technology-Acceptable-Use_update.pdf

[5] Website Privacy policy URL: https://www.lander.edu/about/_files/documents/policies/lp-7_6-website-privacy.pdf

[6] Vulnerability Management policy URL: https://www.lander.edu/about/_files/documents/policies/lp-7_7-vulnerability-management.pdf