LP 7.8

Effective:
5/19/2026

Revised:
6/16/2026

Policy Owner:
Board of Trustees

Policy Administrator:
CITO; Assoc Prov. for AI, Research, Prof. Dev.

Affected Parties:
Employees, students, contractors

Table of Contents:

AI Governance and Responsible Use

1 Purpose and Scope

1.1 This policy and related guidelines establish a shared framework for the responsible use and governance of artificial intelligence (AI) technologies at Lander University. AI tools and systems are increasingly used for teaching, learning, research, administration, communication, and decision-making. For the purposes of this document, AI includes:

- Generative AI tools (e.g., ChatGPT, Copilot, Gemini, Claude)
- Algorithmic decision systems and predictive models
- Other software that performs tasks that usually require human intelligence

1.2 This policy applies to Lander University students, faculty, staff, administrators, contractors, and affiliates, as well as to any AI tool or system used for university work or study, whether provided by the university or accessed through third-party services.

1.3 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”).

2 Guiding Principles

Lander University adopts the following guiding principles for AI use and governance:

2.1 Data Protection and Privacy

2.1.1 Institutional, confidential, or student identifiable data must not be entered into public AI tools unless specifically approved and protected by university contracts and ecosystems.

2.1.2 AI use must comply with the Family Educational Rights and Privacy Act (FERPA); Health Insurance Portability and Accountability Act (HIPAA), where applicable; federal and state laws; and university data and security policies.

2.2 Human-centered Learning and Work

2.2.1 AI should enhance, not replace, faculty instruction, staff expertise, and student learning.

2.2.2 Individual persons remain ultimately responsible for administrative and academic work, official communications, and institutional decisions.

2.2.3 University faculty and staff exercise professional judgment in determining whether and how to use AI in their own teaching, scholarship, assessment, and other work, consistent with department, college, and university guidelines.

2.2.4. Students exercise their own judgments regarding the way in which they engage with AI to support their learning, within the requirements set by their instructors and this policy.

2.3 Academic Integrity and Transparency

2.3.1 Undisclosed or prohibited AI use in coursework or research may be treated as academic misconduct.

2.3.2 When AI assistance is allowed, users must follow course or project requirements for disclosure and attribution.

2.3.3 Faculty must state AI permissions for each course or assignment using one of the following designations: not permitted, permitted for specified tasks with required disclosure, or permitted with attribution. The Office of Academic Affairs will publish standard syllabus language and disclosure templates for each designation.

2.3.4 If a syllabus or assignment does not state whether AI use is permitted, AI use is presumed not allowed for that course or assignment until the instructor states otherwise.

2.3.5 A finding of academic misconduct based on suspected undisclosed AI use must rest on more than a detection tool score. Detection tool output alone is not sufficient evidence of a violation and may not serve as the primary basis for a misconduct finding.

2.3.6 Student work submitted to a third-party AI-detection tool other than university-approved AI-detection tools is an education record subject to FERPA.

Instructors may not submit student work to a tool unless the tool has been reviewed and approved by the institution.

2.4 Critical Evaluation of Output Reliability

AI-generated outputs are shaped by the data, methods, and design choices embedded in the systems that produce them. Those outputs may be incomplete, inaccurate, or unrepresentative of all relevant populations, contexts, or institutional values.

2.4.1 The burden of accuracy and appropriateness rests with the user rather than with the AI system. AI outputs are starting points for human analysis rather than substitutes for it. All AI-users bear a due-diligence responsibility to critically evaluate AI outputs before acting on them, and no AI output should be accepted as authoritative without appropriate human review.

2.4.2 Due Diligence in Evaluating AI Outputs.

Users of AI tools and systems are responsible for critically evaluating all AI outputs prior to use, distribution, or reliance. This due diligence obligation includes:

2.4.2.1 Verifying factual claims and data against authoritative or primary sources.

2.4.2.2 Applying professional judgment, domain expertise, and institutional knowledge when interpreting or acting on AI-generated content.

2.4.2.3 Identifying factual errors, false information, logical inconsistencies, or outputs that appear plausible, but are unsupported.

2.4.2.4 AI users should recognize that AI systems trained primarily on historical or externally sourced data, rather than on current, institution-specific information, may produce outputs that are outdated, biased, or not representative of the university's community or context.

2.5 Human Oversight for High-Impact Institutional Decisions

Given the potential consequences of AI-assisted or AI-informed decision-making at the institutional level, Lander University requires meaningful human review and deliberation for decisions based entirely or in part on AI use that have significant impact on individuals, programs, and/or the university's strategic direction. AI tools may inform analysis and surface patterns, but they should not serve as the sole or determinative basis for high-impact decisions.

2.5.1 Scope of High-Impact Decisions

Human oversight on AI outputs is required at all levels of institutional decision-making, including but not limited to:

2.5.1.1 Individual decisions: Admission, financial aid awards, academic standing, student discipline, hiring, promotion, performance evaluation, and/or termination.

2.5.1.2 Academic and programmatic decisions: Creation, modification, suspension, or elimination of academic programs, majors, certificates, and/or courses.

2.5.1.3 Budget and resource allocation: Significant budget decisions, reallocation of resources, staffing models, and financial planning that affect university operations and/or personnel.

2.5.1.4 Strategic and governance decisions: Institutional planning, policy development, accreditation submissions, Board of Trustees agenda items, presidential priorities, and/or decisions made by cabinet-level administrators.

2.5.2 Responsibilities at Decision-Making Levels

The human oversight obligation applies proportionally across the institution:

2.5.2.1 Frontline staff and faculty must not substitute AI outputs for professional judgment in individual-level decisions.

2.5.2.2 Department chairs, directors, and deans must ensure that programmatic and unit-level decisions involving AI analysis are reviewed with appropriate deliberation and documentation.

2.5.2.3 Vice presidents, cabinet members, and the president bear responsibility for ensuring that institutional and strategic decisions are grounded in verified, contextually sound analyses and not solely in AI-generated summaries, projections, or recommendations.

2.5.2.4 The Board of Trustees should expect that any AI-assisted analysis presented in support of governance decisions has been reviewed, validated, and contextualized by accountable institutional leaders before presentation.

2.6 Transparency and Accountability in AI Systems

2.6.1 Users of AI systems and tools should be transparent about their use of AI when disclosure of use is expected by law, university policy (including course

syllabus requirements), publisher requirements, or the norms of an academic discipline.

2.6.2 Users of AI systems and tools remain accountable for the work product or decisions resulting from the use of AI.

2.7 Innovation and Literacy

2.7.1 The university encourages thoughtful exploration of AI to improve teaching, learning, and operations.

2.7.2 University faculty, staff, and students should enhance their AI literacy, including understanding limitations, hallucinations, bias, and appropriate evaluations of outputs.

3 Acceptable and Prohibited Uses

The examples in this section are illustrative rather than exhaustive. All AI use must comply with the legal requirements in Section 2.1.2 and the disclosure requirements in Section 2.3 of this policy, regardless of whether a specific use appears below.

3.1 Acceptable Use Examples

When consistent with these guidelines and other university policies, acceptable uses of AI include, but are not limited to:

3.1.1 Drafting outlines, brainstorming ideas, or generating practice questions for teaching and learning.

3.1.2 Assisting with computer programming (e.g., code examples, pseudocode, or debugging), with qualified human review of correctness and security.

3.1.3 Summarizing non-confidential documents or public articles to support study or administrative work.

3.1.4 Creating draft accessible materials (e.g., captions, alternative text) subject to human editing.

3.1.5 Supporting low-risk administrative tasks (e.g., draft templates for routine emails) with human review before sending.

3.2 Prohibited Use Examples

When consistent with these guidelines and other university policies, prohibited uses of AI include, but are not limited to:

3.2.1 Entering confidential or restricted institutional data (e.g., Social Security numbers, detailed student records, sensitive HR information, protected health information) into public AI tools.

3.2.2 Using AI to generate or substantially rewrite graded work when the syllabus or assignment prohibits AI assistance.

3.2.3 Relying solely on AI outputs to make high-impact decisions related to:

3.2.3.1 Student admission, financial aid, discipline, or academic standing

3.2.3.2 Employee hiring, promotion, or termination

3.2.4 Using AI to create false or deceptive content (e.g., falsified research data, fabricated references, impersonation, or deepfakes) for academic or institutional purposes.

3.2.5 Deploying AI tools that continuously monitor individuals or process biometrics without appropriate legal, ethical, and institutional review.

4 Roles and Responsibilities

~~4.1~~ Vice Presidents and Cabinet Members

4.1.1 Recommend AI strategy and priorities to the president.

4.1.2 Review proposed institutional AI systems and higher-risk AI projects that use university data or influence decisions about individuals.

4.1.3 Ensure alignment with applicable university policies, federal laws, and state laws (e.g., FERPA, Americans with Disabilities Act [ADA], data security, acceptable use) in consultation with the chief information and technology officer (CITO).

4.1.4 Recommend updates to this policy and guidelines.

4.2 Information Technology Services (ITS)

4.2.1 Evaluates AI-related tools, systems, and vendors for security, accessibility, and data protection.

4.2.2 Maintains a list of approved AI tools and services, including any institutionally licensed AI assistants.

4.2.3 Responds to AI-related security threats and incidents.

4.2.4 Provides and coordinate ITS security and awareness training.

4.2.5 Publishes technical guidance on safe data handling and coordinate integrations with AI and enterprise systems.

4.3 Faculty and Academic Administrators

4.3.1 Clearly state expectations for AI use in syllabi (e.g., prohibited, limited/allowed, or encouraged with attribution).

4.3.2 Design assignments that either meaningfully incorporate AI or make unauthorized AI use less attractive or feasible.

4.3.3 Model responsible AI use and help students critically evaluate AI outputs and recognize bias.

4.4 Students

4.4.1 Follow all course-specific AI rules and seek advice from instructors when expectations are unclear.

4.4.2 Accurately represent their own learning and contributions in assignments, exams, and research.

4.4.3 Evaluate AI outputs critically and verify important information with reliable sources.

4.5 Staff and Administrators

4.5.1 Use AI in ways that support, rather than replace, professional judgment and personal engagement with students and colleagues.

4.5.2 Seek vice president, cabinet member, and ITS reviews and approvals before adopting AI tools, especially those that process student records, HR information, or other institutional data.

5 Data Protection

The classification of data determines the type of data protection required. The university's data classification categories are aligned those of the State of South Carolina data classification scheme and include four definitions (i.e., public, internal, confidential, and restricted).

5.1 PUBLIC

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

5.1.1 Public data may be used with AI tools, provided that copyright and privacy are respected.

5.2 INTERNAL

Internal data includes, but is not limited to, non-public operational information that does not include regulated personal data (e.g., internal memos, draft agendas, training materials, aggregated data, agency procedures, standards).

5.2.1 Internal data may be used only with institutionally approved AI tools and licenses that have appropriate contractual and security safeguards.

5.3 CONFIDENTIAL

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.

5.3.1 Confidential data must not be entered into AI tools unless the service has been explicitly reviewed by ITS and officially acquired by the university.

5.4 RESTRICTED

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.

5.4.1 Restricted data must not be entered into AI tools unless the service has been explicitly reviewed by ITS and officially acquired by the university.

6 AI Tool Selection

6.1 Approved vs Unapproved Tools

6.1.1 ITS will maintain a list of approved AI tools, noting permitted data types and typical use cases.

6.1.2 The university allows the use of third-party AI tools, including user-selected Large Language Models (LLMs), provided that only publicly available information is used. Users must not input or expose confidential, restricted, or non-public university data to these systems.

7 Teaching, Learning, and Syllabus Language

See Lander University's *University Policies in Syllabi* for AI policies related to teaching, learning, and syllabus language:

https://www.lander.edu/about/offices-departments/academic-affairs/university-policies-in-syllabi.html

8 Research and Scholarly Use

8.1 AI tools may not be listed as authors; human researchers remain responsible for content, methodology, and integrity.

8.2 When AI is used in data analysis, translation, or text generation, researchers must document how AI was used and validate outputs.

8.3 Any AI system that processes identifiable human subject data must receive IRB approval and satisfy data protection and security requirements prior to use.

8.4 Researchers must comply with any sponsor or funder-specific restrictions on AI use, including restrictions on AI use in proposal preparation or peer review, in addition to the requirements of this policy. For example, NIH prohibits the use of generative AI in its peer review process and will not consider grant applications substantially developed by AI.

8.5 Grant proposals, manuscripts under review, and other unpublished research materials must not be entered into AI tools that are not institutionally approved under Section 6 of this policy. Submitting unpublished material to a public AI tool may constitute unauthorized disclosure of that material.

8.6 Some research data is restricted by federal law and cannot leave approved systems, even by accident. Entering this kind of data into an AI tool can break that law because the data leaves the researcher's control once it is entered. Researchers must check with their grant's administrator and the Office of Sponsored Projects before using AI with export-controlled or government-restricted data.

9 AI License Requests for Faculty and Staff

To support faculty and staff whose roles significantly benefit from AI use, Lander University will maintain a structured process for requesting institutionally funded AI licenses.

9.1 Guiding Principles for License Allocation

License allocation is guided by:

9.1.1 MISSION ALIGNMENT: With priority to roles that directly support teaching, student success, academic support, university operations, and institutional effectiveness.

9.1.2 DATA STEWARDSHIP: Where possible, licenses should move high-impact users from unapproved consumer tools to secure, institutionally governed tools.

9.2 Request Process

9.2.1 Complete an AI ITS service request ticket that includes name, title, department, and vice president approval.

9.2.1.1 Provide a description of the job duties that would be supported by the requested AI tool.

9.2.1.2 Describe intended uses (e.g., drafting communications, curriculum development, advising support, workflow automation).

9.2.1.3 Indicate whether the work involves student or employee data and, if so, at what sensitivity level.

9.2.1.4 Estimate frequency of use and expected benefits (e.g., time saved, improved quality, new capabilities).

9.2.2 Requests are routed to:

9.2.2.1 The requester's supervisor (including dean or vice president) for initial approval, with additional routing the of the request based on the type of request:

9.2.2.1.1 If the request is a license for an approved AI tool, route the request to ITS for review, prioritization, and final approval to go through appropriate purchasing channels.

9.2.2.1.2 If the request is for a new AI-based system or large project or involves university data with institutional impact, route the request to the vice presidents and/or cabinet member for pre-approval before routing to ITS for review.

9.2.2.2 Certain requests may be submitted by the CITO for review by the State AI Center for Excellence

9.3 Evaluation Criteria

Requests are typically prioritized when they:

9.3.1 Are clearly aligned with student learning, student success, or institutional priorities.

9.3.2 Replace current use of unapproved consumer AI tools with secure institutional tools.

9.3.3 Involve substantial volume or complexity of content where AI can realistically improve efficiency and/or quality.

9.3.4 Include a reasonable, concrete plan for tracking benefits or sharing practices with colleagues.

9.4 Training and Renewal

9.4.1 Approved license-holders must complete basic training on using AI safely and securely before activation. The training is available on Blackboard.

9.4.2 Licenses will be reviewed annually for renewal based on usage, impact, and evolving departmental needs

9.4.3 Underused licenses may be reallocated to other units, with notice to affected users.

10 General AI Purchases and Procurement

To protect university data, manage risks, and ensure responsible use of institutional funds, all AI-related purchases must follow existing procurement and contract policies and these policy and AI guidelines.

10.1 What Counts as an AI Purchase?

10.1.1 Paid licenses or subscriptions for AI tools or services (stand-alone or as add-ons to existing systems).

10.1.2 “Free” or trial versions that require a contract, institutional login, or access to university data.

10.1.3 Cloud services, plug-ins, or integrations that add AI capabilities (e.g., summarization, prediction, chatbots) to current systems.

10.2 Approval and Routing

Before making an AI purchase or accepting an AI-enabled contract or terms of use, employees must complete the following review steps:

10.2.1 Departmental Review

10.2.1.1 The requester obtains supervisor or department chair approval, confirming the purchase supports unit goals and budget.

10.2.1.2 The requester confirms whether the tool will use student, employee, or other institutional data.

10.2.1.3 The AI request will undergo the request process in Section 9.2 of this policy.

10.2.2 ITS and Procurement Review

10.2.2.1 ITS reviews technical, security, and integration implications and confirms whether similar functionality already exists in approved systems.

10.2.2.2 Procurement reviews contracts and terms and approves final purchases.

10.3 Prohibited and Unauthorized Purchases

10.3.1 Individual employees may not independently agree to AI-related terms of use, click through agreements, or initiate data-sharing arrangements on behalf of the university without going through the required approvals.

10.3.2 Use of personal credit cards with later reimbursement to bypass this process is not permitted.

10.3.3 Units must not upload or sync institutional data into unapproved AI tools, even if the tool is “free,” “beta,” or labeled for “educational” use.

10.4 Preferred and Shared Solutions

To avoid fragmentation and reduce risk:

10.4.1 The university will prioritize enterprise or shared AI solutions for use by multiple departments rather than make numerous small, isolated purchases.

10.4.2 Where a centrally approved AI capability already exists, departments are encouraged to use these tools before seeking new, overlapping products.

10.4.3 ITS will periodically publish a list of approved AI tools and recommended use cases, limits, and permitted data types.

11 AI Projects and Pilots

Lander University encourages well-designed AI projects that support innovation in teaching, learning, and operations, while managing risks.

11.1 What Can Be Considered an AI Project?

Examples include, but are not limited to:

11.1.1 A pilot using AI-assisted advising or chatbots for common student questions.

11.1.2 A proof of concept predictive model to identify students who may need additional support.

11.1.3 An AI-supported workflow for automating routine administrative tasks (e.g., form triage, template responses).

11.1.4 A department-level initiative to integrate AI across a sequence of courses.

11.2 Project Proposal Expectations

Before starting a moderate or high-impact AI project, the sponsoring unit or individual must follow the process described in Section 9.2 of this policy to include:

11.2.1 Project title, requestor, description, and team members.

11.2.2 Goals and anticipated benefits.

11.2.3 Description of AI capabilities involved (e.g., text generation, summarization, classification, prediction).

11.2.4 Data to be used, including whether it includes student or employee records and how data will be protected.

11.2.5 Expected scale (e.g., pilot with one program vs campus-wide deployment).

11.2.6 Potential risks and mitigation plans.

11.2.7 How success will be measured and how results will be shared.

11.3 Potential project approval outcomes include:

11.3.1 Proceed as a low risk pilot.

11.3.2 Proceed with conditions (e.g., limited scope, additional training, specific language consent)

11.3.3 Require additional formal review (e.g., IRB, security, accessibility).

11.3.4 Decline or request substantial revision if risks outweigh benefits.

12 Training, Support, and Continuous Improvement

No single Lander University office owns all training and support for AI literacy and training. ITS, the Center for Faculty Excellence, and the university library share this responsibility and will coordinate training and support activities rather than publish separate, uncoordinated guides. Responsibilities for these coordinating areas include:

12.1 Coordination of all training and resources related to AI literacy, safety, and best practices.

12.2 Annual review of all AI-related policies and guidelines, in consultation with university stakeholders, to respond to changing technology, regulations, and campus needs.

13 Related Policies

This policy operates alongside other university policies, including, but not limited to:

- 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)

14 Violations

Any violations of this AI policy may be addressed under applicable student and employee misconduct policies. Any disciplinary action will reflect the nature and impact of the violation.

15 Policy Revision History

- First draft of policy created by Chief Information and Technology Officer on 4/25/2026.
- Prepared for review by Policy Coordinator on 6/2/2026.
- Revised provisional draft approved by Chief Information Technology Officer and AVP for Planning, Analytics and Decision Support on 6/16/2026.
- Stakeholder review and provisional approval of policy on 7/29/2026.
- Final revisions applied by Policy Coordinator on 8/10/2026.
- Reviewed by Board of Trustees Policy Committee on 8/11/2026.
- Approved by the Lander University Board of Trustees on 9/1/2026.