Louisiana Board of Regents
Policy on Responsible, Ethical, and Secure Use of Artificial Intelligence

Adopted: October 22, 2025

I. Policy Statement

The Board of Regents (BOR) recognizes the transformative potential of Artificial Intelligence (AI) to improve BOR's mission to coordinate public postsecondary education in Louisiana in the areas of learning, teaching, research, and administration. However, to realize the potential benefits of AI without risking the possible harm it could cause, AI must be used responsibly and securely across all Louisiana postsecondary education institutions and systems. This AI policy sets forth guidelines to assist in promoting a culture of cybersecurity responsibility and knowledge development within the academic framework for all students, faculty, and staff by BOR and the programs under its jurisdiction, namely the Louisiana Universities Marine Consortium (LUMCON) and the Louisiana Office of Student Financial Assistance (LOSFA). Postsecondary institutions and systems, BOR, LOSFA, and LUMCON must prioritize and promote AI education and discernment to ensure the safety and security of information across data systems and networks. It is imperative that higher education institutions, BOR, and its programs enact appropriate safeguards to ensure integrity in the use of AI as an academic tool, while understanding the shared responsibility necessary to lessen the likelihood of security breaches.

This policy seeks to:

- Prohibit the misuse of AI that undermines data system integrity, privacy, violates data security, or compromises research initiatives;
- Set clear standards for AI use by all staff, consultants, and contractors of BOR and its programs;
- Set clear standards for the enactment of policies governing AI use at postsecondary education institutions in Louisiana;
- Safeguard the confidentiality and integrity of data maintained by BOR and its programs;
- Enable the education of students, faculty, staff and the academic community on the ethical use of AI, the necessity of data and intellectual property protection, and personal responsibility and integrity; and

- Provide for compliance with all applicable laws and this policy and for enforcement in cases of violations in a consistent and timely manner.

II. Introduction

In accordance with its constitutional responsibility to coordinate higher education in Louisiana, the BoR adopts this policy on the Responsible and Ethical use of Artificial Intelligence ("Policy") applicable to BOR and the programs under its jurisdiction, i.e., LOSFA and LUMCON.

III. Definitions

- **Artificial Intelligence (AI) System:** A system engineered and designed to achieve specific objectives, which processes human- or machine-provided inputs and data sources to produce outputs including text, images, audio and other content. The system may also generate predictions, recommendations, and decisions that influence human action and affect real and/or virtual environments. The system can create new content and operate at various levels of autonomy.
- **Institutional Data:** Any data collected, stored, created and/or maintained by a Louisiana public postsecondary institution or a program under BOR oversight. These include, but are not limited to, student data, staff personnel files/records, financial information, and research data.
- **Prohibited Use:** Any use of AI that violates academic integrity, privacy, institutional policy, or applicable state and federal laws and directives, including, but not limited to, unauthorized use or disclosure of sensitive or confidential data, falsification of research data and results, or loading of any proprietary and/or protected data (e.g., student data) into an AI system.

IV. Governance and Oversight

- BOR and each of its programs shall designate a responsible AI officer and AI committee to review AI use proposals, oversee compliance, assess AI tool risk, coordinate with system/institutional counterparts, and maintain an AI use list. BOR shall provide relevant personnel cybersecurity- and AI-related education, focused on authentication of information systems, secure communication across trusted and untrusted networks, data management, internal processes to report safeguard failures, and the function of security operations centers.

V. AI Tools Inventory and Risk Assessment

BOR, through the AI Committee, shall maintain and update regularly an AI tools inventory, which shall include:

- A list of AI tools currently procured, licensed, or approved for use.
- Documentation of each tool's intended use case (academic, research, administrative, communications, fiscal forecast, or cybersecurity).
- Risk classification for each tool (low, medium, high) based on data sensitivity and potential impact.
- Records of vendor compliance reviews, security testing results, and institutional use approval.
- A log of all AI pilot projects, deployments, and decommissioning of AI tools.

VI. Data Privacy, Security and Restrictions

BOR, through the AI Committee, shall establish clear standards to protect sensitive information and prevent unauthorized or harmful use of AI systems, including:

- **Data Classification and Protection:** AI systems may only process institutional data in accordance with existing data classification standards, and state and federal laws. Sensitive personal data (e.g., FERPA, HIPAA, fiscal data, non-public research data) shall not be entered into unapproved internal or external AI tools.
- **Access Control:** AI tool access shall be limited to authorized users using role-based permissions and require multi-factor authentication where applicable and feasible.
- **Data Minimization and Purpose Limitation:** AI tools shall use, collect or process only the minimum data required for their approved use. BOR shall document justification for any sensitive or personally identifiable information (PII) processed by AI systems.
- **Data Retention and Deletion:** BOR and its programs shall establish and enforce defined retention periods for data used in AI systems, with prompt deletion or anonymization carried out in accordance with applicable laws.
- **Source Code and Intellectual Property Restrictions:** AI systems shall not be used to replicate, reverse engineer or disclose proprietary code, trade secrets or intellectual property. To mitigate data leakage, institutions shall explicitly prohibit inputting proprietary institutional software code into unauthorized AI tools.
- **Secure Development and Testing:** AI tools used for development or testing must be sandboxed (isolated within the system) and segmented from production systems

handling sensitive student, finance or research data. BOR and its programs shall maintain audit logs of AI system use to detect misuse or unauthorized access.

- **Cross-Border Data Restrictions:** Institutional data shall not be exported or transmitted to AI systems hosted in jurisdictions without adequate technical and legal protections as approved by the AI Committee.

BOR staff shall be restricted in their use of AI for professional purposes based on the AI tools approved for use. Staff are prohibited from using personal AI accounts on state machines and from conducting state business on any non-state machine. Staff are also prohibited from using a state email address to establish an AI account without written approval of the agency Information Technology department.

VII. Academic Applications

Academic Integrity and Student Use: BOR shall coordinate with all Louisiana postsecondary institutions, through their respective management boards, to ensure: (a) clearly defined permissible and prohibited AI use by students; (b) classroom-level guidelines for responsible AI use, including grading and assessment, by faculty; and (c) methodologies to assess the effectiveness of AI use in teaching and learning.

VIII. Procurement, Vendor Requirements and Third-Party Tools

BOR shall, before adopting or integrating an AI system or related third-party tools, apply the following standards, under which vendors and third-party service providers shall:

- **Risk and Security Assessment:** Comply with National Institute of Standards and Technology (NIST) AI Risk Management Framework, or an equivalent framework, to evaluate data protection, and security.
- **Data Governance:** Define data ownership, retention, deletion rights, and breach notification.
- **Transparency and Documentation:** Maintain AI tool documentation, data flows, compliance reviews and any pilot or testing results.
- **Accessibility:** Comply with state and federal standards for accessibility.
- **Governance Approval:** Comply with governance and oversight requirements as determined by the AI Officer and/or Committee.

IX. Training, Education and Professional Development

- BOR shall implement AI literacy programs to ensure that BOR employees and employees of its programs under its jurisdiction are equipped with knowledge and skills to use AI systems responsibly.
- These trainings shall address, at a minimum, ethics, privacy, attribution of sources, and methods for verifying and validating AI-generated results.
- Specialized training must be offered for security, communications, researchers, and IT staff handling third-party AI integrations.
- Acknowledging the speed of AI development, a review and update of these programs are required on at least a bi-annual basis to assess emerging technologies, risks, state and federal laws, and best practices for the responsible use of AI.

X. Compliance, Reporting and Enforcement

- The AI Committee shall establish procedures to address misuse of AI, including misconduct, data breaches, and unauthorized use and deployment of AI tools, through HR policies, and IT acceptable use policies.
- Data breach or loss shall be reported immediately upon discovery to the AI Officer.
- Non-compliance by employees shall result in the suspension of AI tool usage, revocation of access privileges, and/or the initiation of disciplinary actions.

XI. Review Cycle

This policy shall be reviewed and updated as needed by BOR to reflect emerging risks as well as state and federal law and directives.