



POLICY STATEMENT

NO. 03.37.00

Page 1

COORDINATED BY: FINANCE AND ADMINISTRATION

EFFECTIVE: 11/4/2025

PUBLISHED ONLINE AT:

[Policy Statements \(lsus.edu\)](https://lsus.edu/policy-statements)

SUBJECT: ARTIFICIAL INTELLIGENCE ACCEPTABLE USE

I. PURPOSE

As an institution of higher education, Louisiana State University in Shreveport (“University” or “LSUS”) is charged with maintaining systems and data for administrative, academic, and research purposes. These information assets are critical to the mission of the University, and the acceptable use of these systems and datasets must be managed with formalized Acceptable Use Policies and Standards.

This policy aims to safeguard the University’s data by governing the use of artificial intelligence (AI) systems. It aims to ensure that the use of AI systems complies with the University’s policies and standards which govern data management and to minimize the potential for the unauthorized transfer of data. It further aims to ensure responsible use, protect privacy and security, maintain public trust, support innovation and efficiency, prevent bias and discrimination, and ensure compliance with applicable laws and regulations.

II. SCOPE

This policy applies to all university employees, contractors, and third-party partners who use AI systems in the course of their work for LSUS. It governs the use of AI technologies in any form, including but not limited to machine learning algorithms, automated decision-making systems, generative AI and large language models, and cognitive computing applications. This policy should not be interpreted as superseding existing LSUS policies. Rather, any use of AI systems should operate within existing technology processes and procedures, in addition to the requirements outlined in this policy. LSUS IT Services should be consulted when there is a perceived conflict between this policy and existing LSUS policy.

III. DEFINITIONS

Information Asset – a resource, process, product, information infrastructure, etc. either with a tangible dollar value or whose loss or compromise could intangibly affect its integrity, availability, or confidentiality. The loss or compromise of an information asset could also affect an entity's ability to continue business. Examples of information assets include, but are not limited to, equipment, software, algorithms, and data.

Data – Any information residing on the University IT Infrastructure or held on any other IT Infrastructure on behalf of the University. This data includes but is not limited to files, documents, messages in any format, including e-mail messages and posts made on any Social Media site maintained by/for the University or its units. All data created and/or maintained by a User is also subject to this Policy, even if the data is created and/or stored on the User's own personal computer, smartphone, or other personal device.

User – Any individual or entity that has access to university information assets who falls within the scope of this policy.

Input Data – Any data entered into an AI system for the purpose of generating output. This includes but is not limited to prompts, training data, documents, and instructions.

AI System – Any information asset which has any Artificial Intelligence capabilities or makes use of Artificial Intelligence capabilities directly or indirectly.

Artificial Intelligence (AI) – computer systems capable of performing tasks that typically require human intelligence, including but not limited to machine learning, natural language processing, and computer vision.

Generative AI – tools or systems used to create models that can generate new and original content, such as images, music, or text, based on patterns and examples from existing data.

Deep Learning – model, tool or system used to recognize complex patterns in pictures, text, sounds, and other data to produce insights and predictions.

Machine Learning – computer systems or tools that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.

Ethical AI – AI systems that are designed, developed, and deployed in a manner that is consistent with ethical principles, including fairness, transparency, accountability, and privacy.

Responsible AI – AI systems that are used in a manner that considers the potential social, economic, and ethical implications, and takes steps to mitigate risks and maximize benefits.

Hallucination – A response generated by AI that contains false or misleading information which is presented as fact.

Private Data – Data and/or set of data elements that requires moderate level of security and governance as defined by contractual obligations, University policies, etc., or when unauthorized disclosure, destruction, or modification of such data poses a moderate risk to the University. Appropriate access to Private Data is limited to LSUS employees and non-employees who have a business need-to-know. Examples of Private Data include but are not limited to:

- Information covered by non-disclosure agreements
- Materials for performance of official duties
- Proprietary information of LSUS or others contained within proposals, contracts, or license agreements
- Research data or results that are not confidential data, if classified as such by the Researcher(s)
- Directory Information - a category of personally identifiable information from a student's education record that an institution can disclose without parental or student consent, as long as public notice is given and students have the option to opt-out. This information is considered non-harmful and non-sensitive. Examples of directory information include:
 - Name
 - Mailing address and telephone listing
 - Electronic mail address
 - Date and place of birth
 - Major field of study
 - Grade level
 - Enrollment status (e.g., full-time, part-time)
 - Dates of attendance
 - Participation in officially recognized activities and sports
 - Degrees, honors, and awards received
 - Photograph

Confidential Data – Data and/or set of data elements that requires the highest level of security and governance. Governance of such data is typically driven by regulations (e.g., FERPA, GLBA, HIPAA, etc.) or when unauthorized disclosure, destruction, or modification of such data poses a significant risk to the University. Appropriate access to Confidential Data is limited to only those individuals designated with approved access, signed non-disclosure agreements, and/or a need-to-know. Examples of Confidential Data include but are not limited to:

- Student education records
- Individuals' health records and information (PHI)
- Non-public personal information as it is defined by the Gramm-Leach-Bliley Act (GLBA)
- Research data or results that are confidential data, if classified as such by the Researcher(s), grant sponsor and/or agency
- Prospective student information

- Personally identifiable financial information
- Campus security systems and details
- Credit card numbers
- Certain management information
- Social security numbers
- Government restricted and/or classified information
- Financial transactions of students and employees
- Personnel Records (Although certain records contained within employee personnel files may be “public records” subject to disclosure, personnel files should be maintained as confidential data and disclosure of “public records” shall only be made after a case-by case determination.)

IV. POLICY

A. Guidelines

1. Users may employ AI systems to enhance the efficiency and effectiveness of services provided by the university.
2. Users are prohibited from the following, without prior authorization from LSUS IT Services:
 - i. Entering Private or Confidential data into AI systems.
 - ii. Using AI without supplementing it with human verification to ensure accuracy and factuality to make business decisions including, but not limited to, the following categories:
 - Enrollment
 - Employment
 - Program Eligibility
 - Finances
 - Legal and Regulatory Compliance
 - Law Enforcement
 - Welfare
 - iii. Using AI to bypass security controls (e.g., jailbreaking) or to create, modify, distribute, or execute malicious code.
 - iv. Using AI to create or generate:
 - Illicit content.
 - Content that is unlawful material, or information that lacks broad factual verification or consensus.
 - Spoofs or fraud, including deepfake, impersonation, misinformation, phishing, or social engineering with the intent to harm individuals.

3. Users should review and verify AI input and output for relevance before use to ensure it aligns with its intended purpose and to mitigate risks such as hallucinations, misinformation and bias.
4. AI output used for decision making should be supplemented with human verification to ensure accuracy and factuality. An identified human owner is required to review and approve any AI-assisted output prior to use, and accountability for the decision rests with that designated role.
5. Users should use the “opt-out” option on data collection and model training features that AI systems offer, if available.
6. Users must report the unauthorized use or disclosure of Private or Confidential data in AI systems to LSUS IT Services as soon as possible.
7. Users are required to ensure their use of AI systems complies with LSUS policies, standards, procedures, and all applicable state and federal laws and regulations.

B. Data Governance

1. Users are responsible for ensuring that the use of AI technologies including, but not limited to meeting notetaker tools, complies with the university’s policies, standards, and procedures which govern data management. Users must adhere to established record retention schedules and Louisiana public records laws when utilizing AI generated content. Users should evaluate both AI inputs and outputs for proper data classification and retention before inclusion, dissemination, or deletion.
2. Where applicable, datasets intended for use in AI systems must undergo a documented review prior to deployment. This review shall assess accuracy, completeness, integrity, timeliness, and relevance. Where errors, omissions, duplications, biases, or other deficiencies are identified, appropriate cleansing and remediation measures must be performed before the dataset is approved for use in any AI system.
3. Users must ensure that any sharing of data with AI systems complies with the university’s policies and standards which govern data management.

C. Vetted AI Systems

1. Users shall submit all software, applications, tools, and services which utilize AI for business operations to LSUS IT Services for review and approval prior to procurement, acquisition, or licensure.

2. Users shall ensure that their procurement, acquisition, or licensure of any AI system complies with the university's policies, standards, and procedures which govern the acquisition of information assets as outlined in LSU Permanent Memorandum 50.

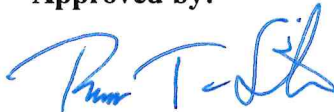
D. Privacy and Security

1. Users must not enter Private or Confidential data into AI systems which do not explicitly protect input data from being trained on by models that can be used by other parties or from being shared with other parties.
2. All AI system use must comply with the university's policies and standards which govern application security, system security, and application acceptable use.

E. Exceptions

1. In limited circumstances, exceptions to this policy may be granted. An exception is defined as a deviation from one or more specific requirements of this policy due to operational necessity, technical limitations, or compelling business needs.
2. Users seeking an exception to this policy must submit a written request to LSUS IT Services. The request must include: The specific policy requirement(s) for which the exception is sought; a clear business justification and description of the operational need; the scope and duration of the requested exception; and a risk assessment and proposed compensating controls.
3. Final approval authority resides with the LSUS Chief Information Officer (CIO) or their designee. Approved exceptions must be documented.

Approved by:



Dr. Robert T. Smith
Chancellor

12/5/25

Date Signed