I. 5.8.33 Acceptable Use of Artificial Intelligence Platforms

Chapter 5 - Information Technology	Original Effective Date: February 2026
Section: 5.8 Information Security	Date Last Reviewed:
Responsible Entity: Chief Information Security Officer	Date Last Revised:

II. Purpose

This policy establishes acceptable use standards for the responsible, ethical, and lawful development and use of Artificial Intelligence (AI) platforms. It promotes innovation while safeguarding academic integrity, privacy, and compliance with relevant state and federal laws.

III. Scope

This policy applies to all faculty, staff, residents, students, contractors, and affiliates who develop, deploy, or interact with AI technologies in their work activities at the institution or on institutional systems. It includes both institution-hosted and third-party AI platforms.

IV. Policy

A. General

1. AI platforms must not be used to process, generate, or transmit sensitive classified data, including but not limited to PHI, PII, intellectual property, or Controlled Unclassified Information (CUI), unless explicitly approved.
2. All AI usage must comply with institutional cybersecurity, privacy, and data classification standards.
3. All AI systems must be documented with responsible ownership, intended use, data sources, and audit requirements.
4. All employees, contractors, and affiliates must complete annual training on responsible AI use.

B. AI Governance and Stewardship

1. A designated AI Governance and Stewardship Committee is responsible for oversight of institutional AI use. The committee shall:

a. Review and approve proposals involving generative AI, automated decision-making, or AI deployed in regulated or sensitive environments.

b. Assess financial, operations, and cyber risk based on data classification, data management standards, and AI model operations.

c. Assess mission and strategic alignment.

d. Establish guardrails, standards, and practices for responsible AI use, including technical and monitoring procedural controls.

e. Authorize pilot programs, specify monitoring and audit requirements, and ensure documentation is maintained.

f. Maintain a risk register for heightened scrutiny AI systems as defined by Texas Administration Code.

g. Recommend corrective actions when AI initiatives present ethical, legal, financial, or operational risks.

C. Transparency and Accountability

1. Institutional investments in AI must align with strategic priorities and undergo Governance Committee review for measurable value and compliance with standards and policies.

2. Consumers must be provided with clear, conspicuous, and timely disclosure when interacting with AI systems, before or at the beginning of the interaction.

3. If an AI system is used in providing health care services or treatment, the provider shall disclose to the recipient of the service or treatment to the recipient's personal representative prior to or at the time care begins, except in emergency situations.

4. Developers of AI systems are responsible for testing and mitigating potential biases, inaccuracies, or discriminatory effects.

5. High-risk AI use cases must be auditable, with logs retained in accordance with UT Health San Antonio policy.

D. Prohibited Activities

1. Using AI to engage in illegal, unethical activities or violate UT Health San Antonio policies.

2. Employing AI to generate or disseminate false or misleading information.

3. Develop or deploy AI systems for the purpose of uniquely identifying a specific individual using biometric data or the targeted or untargeted gathering of images or other media from publicly available sources without the individual's consent if the gathering would infringe on any right of the individual under state or federal laws.

E. Excluded Activities

1. Use of AI to detect, prevent, or respond to security incidents, malware, phishing, identity theft, or fraud.

2. AI used to monitor, investigate, audit, or enforce compliance with institutional, state, or federal regulations.
3. Deployment of AI tools that safeguard IT systems, detect anomalies in performance or function, or preserve the availability and reliability of institutional infrastructure.
4. Use of AI in investigating breaches, misconduct, or other events that threaten security or safety.
5. AI used in emergency healthcare, disaster recovery, or other urgent scenarios where disclosure requirements may be temporarily suspended.

V. Definitions

When used in this document, the following words have the meaning set forth below unless a different meaning is required by context.

Artificial Intelligence – a machine-based systems that, for explicit or implicit objectives, infers, from input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence a physical or virtual environment. These systems may vary in their levels of autonomy and adaptiveness after deployment.

Consequential Decision – a decision that has a material legal or similarly significant effect on the provision, denial, or conditions of a person's access to a government service.

Consumer – an individual who interacts with an AI system in a non-healthcare context, including as part of academic, administrative, or service-based interactions.

Healthcare Recipient – an individual receiving medical care, clinical, or wellness services, including patients or their designated representatives.

Heightened Scrutiny AI System – an AI system that is specifically intended to autonomously make, or be a substantial controlling factor in making, a consequential decision. It does not include systems intended to perform a narrow procedural task, improve the result of a previously completed human activity, perform a preparatory task to an assessment relevant to a consequential decision, or detect decision-making patterns or deviations from previous decision-making patterns.

Machine Learning – a subset of AI where systems learn from data to identify patterns and make decisions with minimal human intervention. ML models evolve over time based on training data and algorithmic processing

Generative AI – AI that generates new content (e.g., text, images, audio, video, simulations).

Large Language Model (LLM) – a type of AI algorithm designed for processing and generating natural language text. LLMs are trained on vast amounts of text data and support applications such as AI chatbots, content creation, and programming assistance.

Principal Basis - the use of an output produced by a heightened scrutiny artificial intelligence system to make a decision with human review, oversight, involvement, or intervention, or meaningful consideration by a human."

VI. Related References

Institutional Handbook of Operating Policies
5.8.10 Information Resources Acceptable Use and Security Policy

5.8.21 Data Classification

Texas Government Code Chapter 522, Regulation of Artificial Intelligence Systems

NIST AI Risk Management Framework

VII. Review and Approval History

The approving authority of this policy is the University Executive Committee.

Effective Date	Action Taken	Approved By	Approved Date
02/27/2026	Policy Origination	Executive Committee	02/27/2026