ILLINOIS TECH

Version	1.0
Date of version:	June 18, 2026
Created by:	CTS
Approved by:	
Confidentiality Level:	INTERNAL USE

ILLINOIS TECH

Table of Contents

Purpose	3
Scope	3
Roles & Responsibilities	3
Policy Controls	3
Responsibility	4
Violation	4
Review	4

ILLINOIS TECH

AI System Security & Risk Management Policy

1. Purpose

This policy established the requirements for managing and securing Artificial Intelligence (AI) systems and applications within the organization. It ensures AI technologies are deployed responsibly, securely, and in alignment with NIST AI Risk Management Framework (AI RMF) and NIST 800-53 control overlays.

2. Scope

- Applies to all AI systems developed, acquired, or deployed by the organization
- Covers the entire AI lifecycle: design, development, training, deployment, monitoring, and retirement.
- Applies to employees, contractors, and third parties with access to the AI system.

3. Roles & Responsibilities

- AI oversight Committee OTS: Governs AI risk, approves deployments, and ensures compliance.
- Developers / Data Scientists (OTS team) : implement secure coding, adversarial testing, and documentation.
- Security Team: Applies NIST SP 800-53 security controls overlay monitoring threats and manages incidents.
- CIO / Business Owner: Ensure AI aligns with organizational goals and ethical standards.

4. Policy Controls

Governance & Risk Management

- All AI projects and applications must undergo risk assessment before deployment.
- Document intended use, limitations, and potential misuse risks.
- Align with Artificial Intelligence Risk Management Framework (AI RMF 1.0) functions: Govern, Map, Measure, Manage.

Data Security & Integrity

- Enforce data source verification and validation to avoid poisoning.
- Encrypt sensitive data in transit and at rest.
- Apply least privilege to control data exposure
- Access control and management
- Apply role-based access controls to training and operational dataset.
- Secure repository with strict access control
- Maintain version control and updates for system and applications

- Frequent / routine coding review for AI systems
- Monitor AI outputs for bias, drift, and anomalies

Operational Safeguards

- Refer to IIT Incident Response Plan manage and respond to AI failures or misuse.
- Require Human-in-the-loop oversight for high-risk decisions.

Compliance & Audit

- Perform annual audits of AI system against NIST AI RMF and SP 800-53 overlays.
- Maintain logs and evidence for accountability and forensic analysis.
- Ensure compliance with applicable laws, regulations, and ethical standards.

Training and Awareness

- Provide mandatory AI security and ethics training for developers, users, and operators.
- Educate faculty, staff and students on emerging AI threats (deepfakes, generative misuse, adversarial attacks).
- Promote a culture of responsible AI use across organization

5. Responsibility

It is the responsibility of Illinois Tech's Data Owners of systems at Illinois Tech to ensure compliance with this policy to the extent of their capabilities, and to hold external vendors working on their behalf accountable.

6. Violations

Illinois Tech investigates and responds to all reports of violations of these and other related policies. Violation of policies will result in disciplinary action in accordance with the Acceptable Use Policy (AUP) and as determined by organizational leadership. If you have any questions about this policy, please contact CTS@illinoistech.edu

7. Review

Review of this policy will be completed on an annual basis or as needed to ensure the applicability of this policy to the changing environment.