INFORMATION TECHNOLOGY POLICY

NUMBER/TITLE: 507 / Security Awareness Training

Covered Individuals: All stakeholders
Covered Locations: All locations
Effective Date: 10/15/2025

Strategic Priority: SP 3
HLC: Criterion 2 & 5
Consultations:

POLICY STATEMENT

All employees are required to complete annual information security training to maintain compliance with university and regulatory data protection standards.

PURPOSE

This policy establishes a framework for educating employees on information security best practices, risks, and responsibilities. Security awareness training ensures employees can identify and respond to threats, safeguard sensitive data, and comply with university and regulatory standards.

DEFINITIONS

PII: Personally Identifiable Information
Social Engineering: Manipulative tactics used to gain confidential information
Insider Threats: Risks posed by individuals within the organization

POLICY IMPLEMENTATION

Upper Iowa University shall provide security awareness training to all employees at least annually, or as required by system changes or updated regulations.

To enhance user awareness, the university will employ training techniques that enable users to:

- Recognize and report indicators of insider threats
- Protect personally identifiable information (PII)
- Identify and report any social engineering attempts

Training content will be reviewed and updated annually, and as needed following security incidents or emerging threats. Lessons learned from internal and external incidents will be integrated to enhance the effectiveness of security awareness training.

To strengthen cybersecurity awareness, ITS may conduct random security simulations such as phishing tests. These exercises help identify risks and improve response readiness. Please stay alert and treat all suspicious activities seriously. Your participation supports a safer digital environment.

Role-Based Security Training

In addition to general security awareness and program-specific training, Upper Iowa University shall provide role-based security training to personnel with responsibilities in software development, systems administration, database administration, and information security. This training must be:

- Assigned prior to system access or commencement of duties, and conducted at least annually thereafter
- Reassigned when roles or systems undergo significant changes
- Updated annually, or in response to major system or role modifications
- Enhanced with lessons learned from internal or external security incidents or breaches

Role-based training ensures that individuals in critical technical and security roles are equipped to manage risks specific to their responsibilities and maintain compliance with institutional and regulatory standards.

Training Records

Upper Iowa University must document and monitor individual information system security training activities including security and privacy awareness training and specific role-based security and privacy training and retain individual training records for at least five (5) years.

Compliance Statement

Failure to complete required training or pass security simulations may result in remediation training. Continued non-compliance may lead to disciplinary action in accordance with university policy. Maintaining security awareness is essential to protecting the university and its data.

CUSTODIAN

Acting as the Policy Owner, the Executive Director of Information Technology Services (ED of ITS) is responsible for answering questions regarding the application of this policy.

RELATED DOCUMENTS, FORMS, AND POLICIES

- ITS Security & Awareness Training Standard Operating Procedure

HISTORY

New/Revision Number	Date of Action/Approval	Revision Change
IT-507	10/15/2025	New