University Policy

Volume I1: Information Technology	**I1.02.5 Information Security** **Effective Date:** 06/15/22 **Last Revised:** **Date of Next Review:** 06/01/27	**Responsible Office:** University Technology Services
Chapter 02: Data Security		**Responsible Officer:** Information Security Officer

POLICY STATEMENT

Northeastern Illinois University (the "University") information and Information Technology Resources (ITR) are essential assets to the success of the University's operations and strategic activities. The University is committed to securing these assets by establishing an information security plan that will enable the implementation of a robust information security management system and foster good security practices within its community.

The Information Security Policy is a key component of the University's information security plan and draws on a framework of best practices. The Information Security Policy is an overarching policy document that provides a strategic overview of the University's information security goals and objectives.

PURPOSE OF THE POLICY

The University's Information Security suite of policies, standards and procedures set the expectations and direction for implementing information security in the University and also provide guidelines to all users of the University's information and IT Resources, including their responsibilities for appropriate use and safety of these assets, and their legal obligations to comply with related statutory requirements.

The objectives of the Information Security Policy are:

- To manage the risks to University information and ITR to an acceptable level.
- To provide and maintain access to University information and ITR to authorized users when needed.
- To adequately protect the University's information and ITR against unauthorized access, accidental loss, misuse, damage, unavailability, or malicious activity.
- To create an awareness culture that informs and reminds users of University information and ITR of their responsibilities for protecting the confidentiality, integrity and availability of these assets, and to comply with the requirements of this policy and related policies.
- To detect and respond to information security incidents promptly and appropriately.
- To improve compliance with relevant audit and statutory requirements.
- To ensure that controls exist and are effective to support the University's business continuity and disaster recovery objectives.

WHO IS AFFECTED BY THIS POLICY

The policy applies to all students, faculty, staff, and all other individuals or organizations who access, use, handle or manage University information and IT Resources.

DEFINITIONS

Authorized Users: All users who are approved to access, handle, process, store, share or manage the University's information and ITR.

Availability: Information and ITR are available to authorized users when required.

Confidentiality: Access to and sharing of sensitive or personal information is restricted only to authorized users based on a valid business need.

Information: A collection of data (paper or digital format).

Integrity: The preservation of the complete, accurate and valid state of information or IT system.

NEIU Information Technology Resources: all electronic and technology facilities, services, devices and data used for information processing, transfer, storage, archiving, display, printing, and communications by NEIU. These include, but are not limited to, networks, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, computing and electronic communications devices and services, modems, email, faxes, telephones, voicemail, video, audio files or recordings, multi-function printing devices, mobile devices, multimedia and instructional materials, and third-party hosted services used to conduct University business. It applies to all devices and communication facilities owned, leased, operated or contracted by the University.

Risk: The probability of an exploited weakness and its resulting consequence leading to an adverse event.

Risk Assessment and Management: The process of identifying and evaluating the likelihood and impact of a risk and implementing mitigating controls to reduce the risk to an acceptable level.

REGULATIONS

815 ILCS 530/ Personal Information Protection Act
Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102
Health Insurance Portability and Accountability Act (HIPAA), P.L. 104-191
5 ILCS 179/ Identity Protection Act
Illinois Social Security Number Protection Task Force Report
Family Educational Rights and Privacy Act, 20 U.S.C. §123

The following principles govern the University's approach for implementing information security:

- The University will implement its information security plan in line with industry best practices and will carry out continuous review and improvement of the plan to strengthen the University's security posture.
- The University will adopt an information security risk management approach that ensures information security risk mitigation efforts reflect the University's risk tolerance level and acceptance.
- University information will be classified and provided with appropriate safeguards commensurate with their value, ensuring they are available when needed and protected against misuse or unauthorized access.
- The University will implement strong access controls to information and ITR, and will carry out periodic reviews of access rights.
- User awareness and training will be provided to the University's community, including end-user awareness and role-specific training.
- The University will implement a robust incident response and management plan to enable prompt and appropriate incident resolution and limit the impact of an incident to the University and its community.
- All relevant contractual, audit, legal and statutory requirements will continue to inform compliance strategies and related activities; and compliance with the Information Security Policies and relevant legislation will be monitored.
- The University will establish and maintain appropriate business continuity and disaster recovery plans to ensure the continuity of its critical operations in the event of a disaster.

APPROACH:

The University will implement its information security plan taking a risk-based approach that identifies the risks to its strategic objectives, defines a plan for mitigating risks and implements relevant controls that leverage best practices and technological solutions to ensure that identified risks are mitigated to an acceptable level, and that the university continues to maintain a strong security posture and satisfy audit, legal and regulatory requirements.

RESPONSIBILITIES:

- The University President's Cabinet oversees the information security plan and has overall responsibility for information security and compliance with related legislation.
- The Office of the Vice President for Finance and Administration has the responsibility for ensuring the provision of resources and support for implementing the information security plan.
- The Information Security Committee has the responsibility for providing strategic leadership and governance of the information security plan and initiatives.
- University Technology Services – Information Security Function has the responsibility for the implementation and management of the information security plan, defining and managing initiatives and associated activities, and monitoring of compliance with the University's Information Security Policies and relevant legislation.

- Students, faculty, staff and other users of university information and ITR have the responsibility for secure and appropriate use and handling of university information and ITR.

ENFORCEMENT:
Any user of the University's information and ITR who violates the Information Security Policies and Procedures may be subject to disciplinary action, which may include removal or restriction of access to prevent any compromise of or damage to University information and ITR, or to protect the University from liability. Unauthorized access or disclosure of information protected by legislation (such as FERPA, IPA, HIPAA, etc.) may result in civil liability or criminal prosecution, up to and including dismissal from the University.

PROCEDURES

There are supplementary policies and procedures for implementing the principles communicated in this policy to achieve its objectives. University Information Security Policies are available on the University's IT Policies page.

GUIDELINES

All users of the University's information and ITR are to be aware of and be current with the University's Information Security Policies and supporting procedures communicated via:

- The University's Information Security Webpages
- Information Security Channel on NEIUport
- UTS Targeted Announcements
- Awareness and Training portal
- Other activities and events to promote information security awareness at the University

AUTHOR REFERENCE

NEIU Information Security Committee

HISTORY

06/15/2022 – Policy Enacted
2021 – Policy Created in Draft Format

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Acceptable Use of Information Technology Resources
ISO 27001 Information Security Management System Codes of Practice

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	Email
Information Security Officer	*(773) 442-4386*	*helpdesk@neiu.edu*

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.