University Policy

Volume I1: Information Technology	**I1.02.6** **Information Security Awareness Training**	**Responsible Office:** University Technology Services
Chapter 02: Data Security	**Effective Date:** 06/30/2022 **Last Revised:** 02/06/2023	**Responsible Officer:** Information Security Officer

POLICY STATEMENT

Information is an essential resource to individuals and organizations for everyday personal activities and job functions. It is important that personal data, work information and IT Resources are used and handled with care to protect them from events that could compromise their confidentiality, integrity, and availability.

Northeastern Illinois University's Information Security Awareness Training Program is designed to educate and train users on best practices for protecting their data, and the university's information and IT Resources they use, to understand their responsibilities for appropriate use and handling of these resources, and to be able to respond to information security threats, risks and incidents appropriately.

PURPOSE OF THE POLICY

The purpose of this policy is to set out the requirement and procedure for information security awareness training for university employees in order to equip them with the knowledge and tools for maintaining information/cyber security at all times to reduce human error and to protect themselves and the University from cyber attacks.

WHO IS AFFECTED BY THIS POLICY

Faculty, staff, and student employees and third-parties who use and/or handle University information and IT resources.

DEFINITIONS

Information Security Awareness Training: This is raising awareness of information security threats and risks, and providing the principles and practices for combating them to keep information and IT resources safe.

Information Security Threat: A malicious act that aims to steal or unlawfully disclose information or disrupt business operations by making information or IT services unavailable to users.

Information Security Risk: This is the probability of an event occurring which could cause significant damage to individuals or organizations through theft, loss or unauthorized disclosure of information, or disruption of an organization's business operations.

REGULATIONS

The University's information security awareness training is mandatory.

Staff and Faculty

- Staff and faculty are required to complete the awareness training course and pass the assessments.
- The awareness training must be completed as soon as the employee can access the University's IT systems or receives a notification to complete the awareness training.
- Additional training may be provided to specific roles as required, i.e., specific privacy training for roles that handle sensitive information as part of their job functions.
- Staff and faculty may be asked to complete additional awareness modules if they have been involved in human error-related incidents that have led to a breach of university information or where information systems have been compromised.

Third Parties

- Third-party agents working with or on behalf of the University are to provide awareness training on information security to their staff if they access the University's information and IT resources.
- Access to the University's information security awareness and training platform may be made available to third-party agents to complete some modules where the University considers it necessary to provide such training.

Enforcement

The University shall determine reasonable completion requirements. Non-compliance with this policy may result in the loss of computing privileges, and/or disciplinary action up to and including termination.

PROCEDURES

Staff and faculty will be automatically registered on the awareness training course and will receive a training notification email.

After receiving the notification email, staff and faculty can access the training platform using their university Net ID and password.

Weekly reminders will be sent to staff and faculty that have incomplete training assignments and may be asked to complete the assignments by a given date where it is necessary to do so.

GUIDELINES

Upon passing the course assessment, a certificate of completion will be issued which users can download or access anytime from the awareness training platform.

It is recommended that staff and faculty complete the optional awareness training modules to learn more about specific security topics, principles and privacy legislation.

Staff and faculty are to familiarize themselves with additional awareness resources available on the University's Information Security webpages.

HISTORY

Drafted June 2022

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Information Security Policy

https://www.neiu.edu/about/university-policy/information-technology

CONTACT INFORMATION

Please direct all questions or concerns about this policy to

Contact	Phone	Email
University Technology Services	(773) 442-4357	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.