INFORMATION SECURITY AWARENESS AND TRAINING POLICY

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-105*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

The Awareness and Training Policy seeks to establish a process to ensure an effective information security awareness and training program throughout the State University of New York at Fredonia (*"Fredonia"*) and its Functional/Business Units. The purpose of an awareness and training program is to educate, document, communicate, and train personnel on information security, information security protocols, best practices, and other information security considerations relevant to the Functional/Business Units' specific function within the institution, the role of the particular employee, and the type of data and system they access and store.

Effective training helps to manage the risks of inadequate information security. For Information Security to be successful and effective in protecting the Information Assets, Business Systems, and Information Technology Resources of Fredonia, all levels of employees and others who access Fredonia's Information Assets and Business Systems must have a full awareness of information security, the relevant policies that apply to those assets, systems, and data sets they utilize for their role at Fredonia, and the importance of adhering to those policies in order to ensure the safety of Fredonia's information.

The Policy is based on the Security and Awareness principles established in NIST SP 800-16 "Information Technology Security Training Requirements: A Role-and Performance-Based Model."

Each Fredonia Functional/Business Unit is bound to follow this policy, and must develop or adhere to a program plan which demonstrates compliance with the requirements of this policy, including documentation that each employee within their Functional/Business Unit has completed the required Information Security training. NOTE: This policy also further supports Fredonia's compliance with the State University of New York Procedures 6900: Information Security Policy which requires all SUNY campuses to provide Annual Security Awareness Training.

The purpose of an information security awareness and training program is to educate, document, communicate, and train personnel on information security, information security protocols, best practices, and other information security considerations relevant to the Functional/Business Units' specific role within the institution, and the type of data and system they access and store.

This process for awareness and training is meant to ensure that information employees and those accessing Fredonia Information Assets, Business Systems, and Information Technology Resources are educated on the importance of information security and the risks of poor information security protocols and processes. This awareness and training will help to protect the Fredonia Information Assets, Business Systems, and

Information Technology Resources, and ultimately, manage the risks of inadequate information security practices of those with access to Fredonia's information and systems.

Each Fredonia Functional/Business Unit utilizing Information Assets, Business Systems, and Information Technology Resources must adhere to the awareness and training process outlined in this Policy, and must develop or adhere to a program plan that demonstrates compliance with the standards enumerated in this Policy.

This policy is applicable to all employees who access Information Technology (IT) Resources owned and/or operated by Fredonia, including Fredonia's Information Assets, Business Systems, and Information Technology Resources. Any information, not specifically identified as the property of other parties, that is transmitted or stored on Fredonia IT Resources (including e-mail, messages and files) is the property of Fredonia. All users of IT Resources, including Fredonia employees, contractors, vendors or others, are responsible for receiving some level of Information security training in accordance with this Policy.

II. POLICY STATEMENT

It is the Policy of Fredonia to establish and adhere to an Awareness and Training process. Each Fredonia Functional/Business Unit utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources, and the employees within each Functional/Business Unit must receive information security awareness and education training so that they can understand the following concepts:

- The underlying significance of security and the specific security related requirements expected of them; and
- The controls, policies and procedures of the Fredonia Security program and the nature of the data they process and store; expected responsibilities and acceptable behaviors need to be clarified, and noncompliance repercussions, which could range from a warning to dismissal, need to be explained before being invoked.

All Fredonia Functional/Business Units must take action to implement the training steps outlined in the NIST SP 800-16 "Information Technology Security Training Requirements: A Role-and Performance-Based Model" standards below in accordance with this Policy. Unless otherwise directed by Federal regulation relating to the implementation of the NIST SP 800-171 requirements, all controls will be implemented in accordance with the "LOW" baseline standard.

1. Security Awareness and Training Policy and Procedures: (AT-1):
   Fredonia:
   a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data and/or systems:
      1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

b. Reviews and updates the current:

1. Security awareness and training policy annually; and
2. Security awareness and training procedures as needed.

2. Security Awareness: (AT-2, 2.2)[1]:

Fredonia provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. Annually thereafter.

Insider Threat (2.2): Fredonia includes security awareness training on recognizing and reporting potential indicators of insider threat.

3. Security Training: (AT-3)[1]:

Fredonia provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. Annually thereafter.

4. Security Training Records Documentation and Monitoring: (AT-4):

Fredonia:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for in accordance with the New York State Records Retention Schedule. .

---

[1] Note: This 800-53 security control directly relates to CUI security requirement 3.2 Awareness and Training specified in the 800-171 document.

III. RELATED DOCUMENTS, FORMS AND TOOLS

SUNY Procedure, Information Security Guidelines, Procedure Document 6608.

OTHER RELATED INFORMATION

The following are references to related Federal and State laws, policies, guidelines, and resources on cyber security.

Federal NIST National Institute of Standards and Technology, U.S. Department of Commerce, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center.

- NIST 800-53
  - NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, Joint Task Force Transformation Initiative, April 2013.
    - Summary: To achieve more secure information systems and effective risk management, document provides "guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems."
  - Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Computer Security Division, February 19, 2014.
    - Summary: Provides an overview of NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, which was published April 30, 2013.
  - NIST Special Publication 800-53, NIST SP 800-53 database of security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations.
    - Security Controls and Assessment Procedures for Federal Information Systems and Organizations - Control Families, NIST Special Publication 800-53 (Rev. 4).
      - AC - Access Control
      - AU - Audit and Accountability
      - AT - Awareness and Training
      - CM - Configuration Management
      - CP - Contingency Planning
      - IA - Identification and Authentication
      - IR - Incident Response
      - MA - Maintenance
      - MP - Media Protection
      - PS - Personnel Security

- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

- NIST 800-50
  - Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, United States Department of Commerce National Institute for Standards and Technology (NIST), October 2003.
- NIST 800-16
  - Special Publication 800-16, Information Security Training: A Role-Based Model for Federal Information Technology/Cybersecurity Training, United States Department of Commerce National Institute for Standards and Technology (NIST), March 2014.
- NIST 800-12
  - Special Publication 800-12, An Introduction to Computer Security: the NIST Handbook, United States Department of Commerce National Institute for Standards and Technology (NIST), October 1995.
- NIST 800-100
  - Special Publication 800-100, Information Security Handbook: A Guide for Manager, United States Department of Commerce National Institute for Standards and Technology (NIST), October 2006.
- NIST 800-171
  - NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015.

New York State

- New York State Information Technology Policy Number: NYS-P03-002, Information Security Policy.
  - Available at: https://its.ny.gov/sites/default/files/documents/enterprise_information_security_policy_v5.1_0.pdf

IV. DEFINITIONS

TERM	DEFINITION
Business Systems	Any and all Information Technology (IT) resources and information assets owned and/or operated by Fredonia.
Functional/ Business Unit	This term used throughout the policy refers to each and every functional, department, and office unit within Fredonia, from the Provost area, to HR, to Finance, to the Business Office, to ITS, and on and on.
Information Asset	This term used throughout the policy refers to Fredonia's information assets. Fredonia creates, possesses, and manages information. This information is Fredonia property with a financial value. The term "information asset" refers to the information that Fredonia has in its possession that had value to the institution. That value of information increases based on the value that the information has to Fredonia, both as property, and as a tool to allow Fredonia to operate its Information Assets, Business Systems, and Information Technology Resources and Functional/ Business units.
Information Technology (IT) Resources	This term used throughout the policy refers to Fredonia's information assets (i.e. hardware, software, or data). Fredonia creates, possesses, and manages information. This information is Fredonia property with a financial value. The term "Information Resources" refers to the information that Fredonia has in its possession that had value to the institution. That value of information increases based on the value that the information has to Fredonia, both as property, and as a tool to allow Fredonia to operate its Business Systems and Functional/ Business units.
Event and/or Transaction	For purposes of this Policy, an "event" or "transaction," at a minimum, will always include the following: ● User Access within a Business System ● User Transactions with respect to access of Information Assets, Business Systems, and Information Technology Resources ● Any technology access events or transactions specifically designated by the Functional/Business Unit as a circumstance which rises to the level of an "event" or "transaction" worthy of documentation in the form of access logs, documented access transactions, or other access to information assets that is recorded for purposes of audit and accountability.

V. CONTACT & ENFORCEMENT

ROLE	CONTACT	PHONE	EMAIL - Website
Responsible Office	Information Technology Services	(716) 673-3407	tracker@fredonia.edu
Enforcement	Human Resources	(716) 673-3434	human.resources@fredonia.edu
Policy	University Policy Office	(716) 673-4828	policy@fredonia.edu policy.fredonia.edu