FREDONIA
STATE UNIVERSITY OF NEW YORK

Information Security Incident Response Policy

policy.fredonia.edu

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-108*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

The State University of New York at Fredonia (*"Fredonia"*) Information Security Response Policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this Policy to establish an incident response capability throughout Fredonia and its Functional/Business units for identifying, responding to and managing Information Security incidents which may occur across the enterprise environment. The capability is meant to remediate any Information Security Risks which are realized.

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 standards enumerated within the Policy.

This Policy establishes the Fredonia Information Security Incident Response Policy. This Policy is designed to support risk mitigation activities that stem from computer security incidents, by establishing of an Enterprise Incident Response capability. In addition, it supports the incident management program and is one of four key Enterprise IT security practices that detect, analyze, prioritize and handle Information Security Incidents which may occur within Fredonia.

This Policy is applicable to all Information Assets, Business Systems, and Information Technology Resources owned and/or operated by Fredonia. 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 adhering to this Policy.

II. POLICY STATEMENT

It is the Policy of Fredonia to establish and adhere to an Incident Response Policy that ensures security best practices and capabilities throughout Fredonia and its business units. The primary goal is to identify and manage the risks associated with information security incidents. Such incidents include any malicious act or suspicious event that: compromises, or was an attempt to compromise, the electronic or physical security of a critical information technology asset; or, disrupts, or was an attempt to disrupt, the operation of Fredonia information systems or assets. This includes unauthorized access, or authorized access for inappropriate purposes, that may intentionally or unintentionally render Fredonia systems unsecure. Each Fredonia Functional/Business Unit utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources must adhere to the Incident Response Policy, and must develop or adhere to a program plan that demonstrates compliance with the standards enumerated in this Policy.

All Fredonia Functional/Business Units must take action to implement the Identification and Authentication steps outlined in the NIST SP 800-53 “Identification and Authentication Family guidelines” 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.

NOTE: The Information Technology Services (ITS) department will generally be the primary implementers of these controls however, any employee or affiliate utilizing University regulated data and/or system(s) will need to adhere to the policy requirements.

1. Incident Response Plan: (IR-1):
    Fredonia through its Information Security Committee:
    a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data and/or systems:
        1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
    b. Reviews and updates the current:
        1. Incident response policy annually; and
        2. Incident response procedures as needed.
2. Incident Response Training: (IR-2)[1]:
    Fredonia through its Information Security Committee provides incident response training to information system users consistent with assigned roles and responsibilities:
    a. Within 30 days of assuming an incident response role or responsibility;
    b. When required by information system changes; and
    c. Annually thereafter.
3. Incident Response Testing and Exercise: (IR-3)[1]:
    Fredonia Incident Response Team (FIRT) tests the incident response capability for the information system annually using the use of checklists, walk-through or tabletop

exercises, simulations (parallel/full interrupt), and comprehensive exercises to determine the incident response effectiveness and documents the results.

Coordination With Related Plans (3.2):

FIRT coordinates incident response testing with organizational elements responsible for related plans.

4. Incident Handling: (IR-4)[1]:

Fredonia:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

5. Incident Monitoring: (IR-5)[1]:

Freodnia tracks and documents information system security incidents.

6. Incident Reporting: (IR-6)[1]:

Fredonia:

a. Requires personnel to report suspected security incidents to the organizational incident response capability as soon as possible or within ; and

b. Reports security incident information to Chief Information Security Officer at security@fredonia.edu or (716) 673-4725.

7. Incident Response: (IR-7)[1]:

Fredonia provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

[1] Note: This 800-53 security control directly relates to CUI security requirement 3.6 Incident Response 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 800-171
    - NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015.
- NIST 800-83 Rev 1
    - NIST Special Publication 800-83 Rev 1, Guide to Malware Incident Prevention and Handling, July 2013.
- NIST 800-61 Rev 2
    - NIST Special Publication 800-61 Rev 2, Computer Incident Handling Guide, August 2012.

New York State

- New York State Cyber Incident Reporting Procedures.
- New York State Information Technology Standard Number: NYS-S13-005, Cyber Incident Response Standard.
    - Available at: https://its.ny.gov/document/cyber-incident-response-standard

Fredonia

- State University of New York Procedure Number: 6608, Information Security Guidelines - Campus Programs & Preserving Confidentiality.
    - Available at: https://www.suny.edu/sunypp/documents.cfm?doc_id=583
- State University of New York Cyber Incident Reporting Procedure, update 2016

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 IT, Counsel's Office, 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 has 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 has 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