FREDONIA
STATE UNIVERSITY OF NEW YORK

SYSTEM & INFORMATION INTEGRITY POLICY

policy.fredonia.edu

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-110*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

The Systems and Information Integrity Policy requires that the State University of New York at Fredonia (*"Fredonia"*) Functional/Business Units respective Business Systems, Information Assets, Information Technology (IT) Resources, and information are managed in an effective manner to ensure the integrity of the systems and information in Fredonia's possession. This Policy seeks to establish a process to manage the risks that originate from system flaws and vulnerabilities, malicious code, unauthorized code changes, and inadequate management of a system error through an established and effective System and Information Integrity program.

The System and Information Integrity Policy sets the expectation that the systems used during our day-to-day business, as well as the information (i.e., data) that we produce, handle, or otherwise maintain within these systems are valid, trustworthy, reliable, and uncompromised.

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.

This Policy is based on the System and Information Integrity principles established in NIST SP 800-53 "System and Information Integrity," Control Family guidelines.

An adequate System and Information Integrity Program helps Fredonia to ensure that the information throughout Fredonia and its Functional/ Business units is a true and accurate representation of Fredonia's data so that the data maintains its integrity. Fredonia as an organization must implement security standards for system configuration, data protection, and system-correcting error handling in order to ensure the information and data is correct, and has not been compromised through system handling error or some secondary action.

This Policy is applicable to all employees who access Information Technology (IT) Resources owned and/or operated by Fredonia, including Fredonia's Business Systems and Information Assets. 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 a System and Information Integrity Policy to manage the risks that originate from system flaws and vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling. An adequate System and Information Integrity program helps Fredonia to ensure adequate system configuration, system security, and error handling. System and Information Integrity is a foundational expectation that the systems used during our day-to-day business, as well as the information (i.e., data) that we produce, handle, or otherwise maintain within these systems are valid, trustworthy, reliable, and uncompromised. It is incumbent on every Fredonia employee to guarantee that our Business Systems, Information Assets, IT Resources, and information retain and maintain a level of accuracy such that Fredonia can maintain a level of confidence in the data that it relies upon.

All Fredonia Functional/Business Units must take action to implement the training steps outlined in the NIST SP 800-53 “System and Information Integrity,” Control 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. System and Information Integrity Procedures: (SI-1):
   Fredonia:
   - a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data and/or systems:
     - 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
     - 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
   - b. Reviews and updates the current:
     - 1. System and information integrity policy annually; and
     - 2. System and information integrity procedures as needed.
2. Flaw Remediation: (SI-2)[1]:
   Fredonia:
   - a. Identifies, reports, and corrects information system flaws;
   - b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
   - c. Installs security-relevant software and firmware updates within 30 days of the release of the updates or sooner; and
   - d. Incorporates flaw remediation into the organizational configuration management process.

3. Malicious Code Protection: (SI-3) [1]:

Fredonia:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

1. Perform periodic scans of the information system as needed and real-time scans of files from external sources at the; endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

2. Block malicious code; quarantine malicious code; send alert to administrator; an alert in response to malicious code detection; and

d.Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

4. Information System Monitoring: (SI-4) [1]

Fredonia:

a. Monitors the information system to detect:

1. Attacks and indicators of potential attacks; and

2. Unauthorized local, network, and remote connections;

b. Identifies unauthorized use of the information system through scans, log analysis, and other industry standard practices;

c. Deploys monitoring devices:

1. Strategically within the information system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g. Provides appropriate information system monitoring information to law enforcement, executive leadership, and intelligence organizations as needed.

5. Security Alerts, Advisories, and Directives: (SI-5) [1]:

Fredonia:

a. Receives information system security alerts, advisories, and directives from law enforcement and intelligence agencies on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to appropriate personnel.

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

6. Security Functionality Verification: (SI-6):

Fredonia:

a. Receives information system security alerts, advisories, and directives from law enforcement information, intelligence information, or other credible sources of information on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to:law enforcement information, intelligence information, or other credible sources of information; and

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

7. Software and Information Integrity: (SI-7):

Fredonia employs integrity verification tools to detect unauthorized changes to specific software, firmware, and information.

8. Spam Protection: (SI-8):

Fredonia:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

9. Information Input Restrictions: (SI-9): [Withdrawn]

10. Information Input Validation: (SI-10):

The information system checks the validity of information inputs.

11. Error Handling: (SI-11):

The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

b. Reveals error messages only to approved personnel.

12. Information Output Handling and Retention: (SI-12):

Fredonia handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

[1] Note: This 800-53 security control directly relates to CUI security requirement 3.14 System and Information Integrity 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 800-92
    - Special Publication 800-92, Guide to Computer Security Log Management, United States Department of Commerce National Institute for Standards and Technology (NIST), September 2006.
- NIST 800-94 Rev 1
    - Special Publication 800-94 Rev 1, Guide to Intrusion Detection and Prevention Systems (IDPS), United States Department of Commerce National Institute for Standards and Technology (NIST), July 2012.
- NIST 800-45 Version 2
    - Special Publication 800-45 Version 2, Guidelines on Electronic Mail Security, United States Department of Commerce National Institute for Standards and Technology (NIST), February 2007.
- NIST 800-61 Rev 2
    - Special Publication 800-61, Computer Security Incident Handling Guide, United States Department of Commerce National Institute for Standards and Technology (NIST), August 2012.

- NIST 800-40 Rev 3
    - Special Publication 800-40 Rev 3, Creating a Patch and Vulnerability Management Program, United States Department of Commerce National Institute for Standards and Technology (NIST), November 2005.
- NIST 800-83 Rev 1
    - Special Publication 800-83 Rev 1, Guide to Malware Incident Prevention and Handling, United States Department of Commerce National Institute for Standards and Technology (NIST), July 2015.
- 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 Standard Number: NYS-S15-001, Patch Management Standard.
    - Available at: https://its.ny.gov/document/eiso/patch-management-standard
- New York State Information Technology Standard Number: NYS-S14-008, Secure Configuration Standard.
        - Available at: https://its.ny.gov/document/secure-configuration-standard

IV. DEFINITIONS

TERM	DEFINITION
Business Systems	Any and all Information Technology (IT) resources and information assets owned and/or operated by Fredonia.
Systems Custodian	
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 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 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