Information System Maintenance Policy

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-111*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*

I. REASON FOR POLICY

This Information Systems Maintenance Policy establishes a process for managing risks from information asset maintenance and repairs through the establishment of an effective System Maintenance program. The system maintenance program helps the State University of New York at Fredonia ("Fredonia") implement security best practices with regard to enterprise system maintenance and repairs.

The Fredonia Information Systems Maintenance Policy serves to be consistent with best practices associated with organizational Information Security management. This Policy establishes the requirement of an information systems maintenance management process throughout Fredonia and its Functional/Business Units. The system maintenance program helps Fredonia implement security best practices with regard to enterprise system maintenance and repairs.

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.

An adequate Information Systems Maintenance process helps Fredonia manage the risks associated with known hardware and software vulnerabilities relating to Fredonia system assets, will aid in the proper management and monitoring of such assets, and is a key component relating to information system update/upgrade processes. This Policy establishes the requirement of an information systems maintenance process throughout Fredonia and its Functional/Business Units to help the organization ensure adherence to industry best practices regarding its information assets.

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 information systems maintenance process that ensures security best practices and capabilities throughout Fredonia and its Functional/Business units. The purpose of an information systems maintenance process is to help manage the risks associated with both hardware and software maintenance. Failure to follow well defined and well documented maintenance procedures relating to both information system software and hardware poses a significant risk to the organization and may place critical systems and sensitive data are risk. It is the intention of this Policy to establish a system maintenance capability throughout Fredonia and its Functional/Business units to help the organization implement security best practices with regard to enterprise information system maintenance and repairs. Each Fredonia Functional/Business Unit utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources must adhere to the information system maintenance process outlined in this 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. Information Systems Maintenance Policy and Procedures: (MA-1):
   Fredonia:
   a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data and/or systems:
      1. A system maintenance 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 maintenance policy and associated system maintenance controls; and
   b. Reviews and updates the current:
      1. System maintenance policy annually; and
      2. System maintenance procedures as needed.
2. Controlled Maintenance : (MA-2)[1]:
   Fredonia:
   a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
   b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that Fredonia Information Technology Services systems custodian or Department Head explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Includes at minimum the systems serial number, manufacturer, model, SUNY Fredonia Asset Tag, Computer Name (if applicable), item description, security category and temporary location in organizational maintenance records.

3. Maintenance Tools: (MA-3, 3.1, 3.2)[1]:

Fredonia approves, controls, and monitors information system maintenance tools.

Inspect Tools (3.1): Fredonia inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications

Inspect Media (3.2): Fredonia checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

4. Nonlocal Maintenance: (MA-4)[1]:

Fredonia:

a. Approves and monitors nonlocal maintenance and diagnostic activities;

b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintains records for nonlocal maintenance and diagnostic activities; and

e. Terminates session and network connections when nonlocal maintenance is completed

5. Maintenance Personnel: (MA-5)[1]:

Fredonia:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

6. Timely Maintenance: (MA-6):

Fredonia obtains maintenance support and/or spare parts for campus technology in accordance with established Service Level Agreements and Maximum Tolerable Downtime (MTD) associated with the given service.

---

[1] Note: This 800-53 security control directly relates to CUI security requirement 3.7 Maintenance 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.

New York State

- New York State Information Technology Policy Number: NYP-P03-002, Information Security Policy.
  - Available at: https://its.ny.gov/document/information-security-Policy
- New York State Information Technology Standard Number: NYS-S15-005, Patch Management Standard.
  - Available at: https://its.ny.gov/document/eiso/patch-management-standard
- New York State Information Technology Standard Number: NYS-S15-002, Vulnerability Scanning Standard.
  - Available at: https://its.ny.gov/document/eiso/patch-management-standard

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 is 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