Configuration Management Policy

policy.fredonia.edu

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-106*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

This Configuration Management Policy establishes a process to ensure an effective configuration management program designed to help manage the risks from system changes impacting baseline configuration settings, system configuration, and security.

The State University of New York at Fredonia (*"Fredonia"*) Configuration Management Policy serves to be consistent with best practices associated with organizational Information Security management. This Policy establishes the requirement of a configuration management process throughout Fredonia and its Functional/Business Units. The configuration management program helps Fredonia document, authorize, manage and control system changes impacting its Information Systems.

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 is based on the Configuration Management principles established in NIST SP 800-53 "Configuration Management Family guidelines."

An adequate Configuration Management process helps Fredonia manage the risks of inadequate configuration change management monitoring and to aid in the proper retention of audit evidence. This Policy establishes the requirement of a configuration management process throughout Fredonia and its Functional/Business Units to help the organization ensure that there is adequate configuration change management documentation (logging), and the retention of audit evidence for purposes of demonstrating efforts related to information system modifications.

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 a Configuration Management process that ensures that established information systems configuration baselines are followed and that any configuration modifications to information systems are adequately documented/logged. The purpose of a Configuration Management process is to help manage the risks associated with undocumented or unauthorized modifications to existing information systems. Such unmanaged modifications may intentionally or unintentionally render Fredonia systems less secure and make retention of audit evidence difficult. Each Fredonia Functional/Business Unit utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources must adhere to the configuration management 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 Configuration Management steps outlined in the NIST SP 800-53 "Configuration Management 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. Configuration Management Policy and Procedures: (CM-1):
    Fredonia:
        a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data and/or systems:
            1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
            2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
        b. Reviews and updates the current:
            1. Configuration management policy annually; and
            2. Configuration management procedures as needed.
2. Baseline Configuration: (CM-2)[1]:
    Fredonia develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
3. Configuration Change Control: (CM-3)[1]:
    Fredonia:
        a. Determines the types of changes to the information system that are configuration-controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system in accordance with the New York State Records Retention Schedule;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through an appropriate supervisor or committee that convenes at least weekly if necessary to review changes.

4. Security Impact Analysis: (CM-4)[1]:

Fredonia analyzes changes to the information system to determine potential security impacts prior to change implementation.

5. Access Restrictions for Change: (CM-5)[1]:

Fredonia defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

6. Configuration Settings: (CM-6)[1]:

Fredonia:

a. Establishes and documents configuration settings for information technology products employed within the information system using (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

7. Least Functionality: (CM-7: 7.1, 7.2, 7.4, 7.5)[1]:

Fredonia:

a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the functions, ports, protocols, and/or services to ensure only that which is required is permitted to proper use of the system.

Periodic Review (7.1):

Fredonia:

(a) Reviews the information system in accordance with implementations, upgrades and annually to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
(b) Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.

Prevent Program Execution (7.2): The information system prevents program execution in accordance with Fredonia Acceptable Use Policy.

Unauthorized Software / Blacklisting (7.4):

Fredonia:

(a) Identifies programs not approved by ITS ;

(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

(c) Reviews and updates the list of unauthorized software programs at least annually and as necessary.

Authorized Software / Whitelisting (7.5):

Fredonia:

(a) Identifies software programs from ITS approved software list and approved standard configurations for workstations, laptops, and other mobile devices;

(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

(c) Reviews and updates the list of authorized software programs at least annually and as necessary.

8. Information System Component Inventory: (CM-8: 8.1)[1]:

Fredonia:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;

2. Includes all components within the authorization boundary of the information system;

3. Is at the level of granularity deemed necessary for tracking and reporting; and

4. Includes hardware inventory specifications, software license information, software version numbers, data security category, component owners, and for networked components or devices, machine names and network addresses; and

b. Reviews and updates the information system component inventory to include information system manufacturer, device type, model, serial number, data security category, and physical location.

Updates During Installations / Removals (8.1):

Fredonia updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

9. Configuration Management Plan: (CM-9):

Fredonia develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the information system and places the configuration items under configuration management; and

d. Protects the configuration management plan from unauthorized disclosure and modification.

10. Software Usage Restrictions: (CM-10):

Fredonia:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

11. User Installed Software: (CM-11)[1]:

Fredonia:

a. Establishes software defined policies governing the installation of software by users;
b. Enforces software installation policies through Information Technology Services (ITS) office; and
c. Monitors policy compliance at least annually and as necessary.

---

[1] Note: This 800-53 security control directly relates to CUI security requirement 3.4 Configuration Management 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 800-171
  - NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015.
    - Summary: The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations. The requirements apply to all components of nonfederal information

systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and non-federal organizations.

- NIST 800-128
  - Special Publication 800-128, Guide for Security Configuration Management of Information Systems, United States Department of Commerce National Institute for Standards and Technology (NIST), August 2011.
    - Summary: this publication provides guidelines for implementation of the Configuration Management family of security controls defined in NIST SP 800-53 (CM-1 through CM-9). This publication also includes guidelines for NIST SP 800-53 security controls related to managing the configuration of the information system architecture and associated components for secure processing, storing, and transmitting of information. Configuration management is an important process for establishing and maintaining secure information system configurations, and provides important support for managing security risks in information systems.

- 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.
    - Summary: Written for the federal sector, but provides guidance on a variety of other governmental, organizational, or institutional security requirements. Within the document, it informs information security management teams (CIOs, CISOs, and security managers) about various aspects of information security that they will be expected to implement and oversee in their respective organizations, and provides guidance for facilitating a more consistent approach to information security programs across the federal government.

- 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.
    - Summary: Assists organizations in understanding the need for sound computer security log management and provides practical guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise.

- NIST 800-60
  - Special Publication 800-60 Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories, United States Department of Commerce National Institute for Standards and Technology (NIST), August 2008.
    - Summary: The guideline's objective is to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system.

- 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 800-40
  - Special Publication 800-40 Revision 3: Creating a Patch and Vulnerability Management Program, United States Department of Commerce National Institute for Standards and Technology (NIST), November 2013.
    - Summary: This publication is designed to assist organizations in understanding the basics of enterprise patch management technologies. This publication is based on the assumption that the organization has a mature patch management capability and is focused on increasing its automation level. Organizations that are seeking more basic guidance on establishing patch management programs or have legacy needs that cannot be met with current enterprise patch management technologies should, in addition to reading this publication, also consult the previous complementary version, NIST SP 800-40 Version 2, Creating a Patch and Vulnerability Management Program.

New York State

- New York State Information Technology Standard Number: NYS-S14-005, Security Logging Standard.
  - Available at: https://www.its.ny.gov/document/security-logging-standard.
- New York State Information Technology Standard Number: NYS-S14-008, Security Logging 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.
Functional/Business Unit	This term used throughout the Policy refers to each and every functional, department, and office unit within Fredonia.
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