Media Protection Policy

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-109*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

This Media Protection Policy establishes a process for managing risks from media access, media storage, media transport, and media protection through the establishment of an effective Media Protection program.

The State University of New York at Fredonia ("Fredonia") Media Protection Policy serves to be consistent with best practices associated with organizational Information Security management. This Policy establishes the requirement of a Media Protection management process throughout Fredonia and its Functional/Business Units. This program helps Fredonia implement security best practices with regard to any type of computer information system related media usage, storage, and disposal associated with Fredonia information assets.

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 Media Protection principles established in NIST SP 800-53 "Media Protection Family Guidelines."

An adequate Media Protection process helps Fredonia manage the risks of improper media usage, storage and disposal and will aid in the proper management and monitoring of such assets. This Policy establishes the requirement of a Media Protection process throughout Fredonia and its Functional/Business Units to help ensure that the organization adheres to industry best practices regarding Media Protection for Fredonia information assets.

This Policy is applicable to all Information Assets, Business Systems, and Information Technology Resources owned and/or operated by Fredonia. Any media, 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 Media Protection process that ensures security best practices and capabilities throughout Fredonia and its Functional/Business units. The purpose of a Media Protection process is to help manage the risks associated with inappropriate media usage, storage and disposal. Proper Media Protection is critical for ensuring that Fredonia systems have not been compromised. Each Fredonia Functional/Business Unit or Affiliate utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources must adhere to the Media Protection 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 Media Protection steps outlined in the NIST SP 800-53 “Media Protection Family guidelines” in accordance with this Policy. Unless otherwise directed by Federal regulations 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. Media Protection Policy and Procedures: (MP-1):
   Fredonia:
   - a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data and/or systems:
     - 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
     - 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
   - b. Reviews and updates the current:
     - 1. Media protection policy annually; and
     - 2. Media protection procedures as needed.
2. Media Access: (MP-2)[1]:
   Fredonia restricts access to Universal Serial Bus (USB) external drives other such external media drives to Category III - Restricted computers.
3. Media Marking: (MP-3)[1]:
   Fredonia:
   - a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
   - b. Exemption are made on a case by case basis and need the approval of the Information Security Office (ISO).
4. Media Storage: (MP-4)[1]:
   Fredonia:

a. Physically controls and securely stores digital and/or non-digital media within locked areas at all times; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

5. Media Transport: (MP-5: 5.4)[1]:

Fredonia:

a. Protects and controls electronic and physical media containing regulated University data while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. “Electronic media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or

2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

Fredonia personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.

2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

Fredonia personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.

2. Limiting the collection, disclosure, sharing and use of Fredonia regulated data.

3. Following the least privilege and role based rules for allowing access. Limit access to Fredonia regulated data to only those people or roles that require access.

4. Securing hand carried confidential electronic and paper documents by:

a. Storing Fredonia regulated data in a locked briefcase or lockbox.

b. Only viewing or accessing the Fredonia regulated data electronically or document printouts in a physically secure location by authorized personnel.

c. For hard copy printouts or Fredonia regulated documents:

i. Package hard copy printouts in such a way as to not have any Fredonia regulated information viewable.

ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing Fredonia regulated information material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

5. Not taking Fredonia regulated data home or when traveling unless authorized by your supervisor or . When disposing of confidential documents, use a cross-cut shredder.

b. Maintains accountability for information system media during transport outside of controlled areas;

c. Documents activities associated with the transport of information system media; and

d. Restricts the activities associated with the transport of information system media to authorized personnel.

Cryptographic Protection (5.4): The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

6. Media Sanitization: (MP-6)[1]:

Fredonia:

a. Sanitizes electronic storage media prior to disposal, release out of organizational control, or release for reuse using methods approved by the Information Security Office (ISO) in accordance with applicable federal and organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

7. Media Use: (MP-7: 7.1)[1]:

Fredonia prohibits the use of external storage media (e.g USB hard drives) on Category III - Restricted computers.

Prohibit Use Without Owner (MP-7.1):

Fredonia prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

8. Media Downgrading: (MP-8):

Fredonia:

a. Establishes information system media downgrading process approved by the Information Security Office (ISO);

b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;

c. Identifies information system media requiring downgrading; and

d. Downgrades the identified information system media using the established process.

[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 800-53
  - 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 800-100
    - 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 800-76-2

- Special Publication 800-76-2 Biometric Data Specification of Personal Identity Verification, United States Department of Commerce National Institute for Standards and Technology (NIST), July 2013.
  - Summary: This document contains technical specifications for biometric data mandated or allowed in [FIPS]. These specifications reflect the design goals of interoperability, performance and security of the PIV Card and PIV processes. This specification addresses iris, face and fingerprint image acquisition to variously support background checks, fingerprint template creation, retention, and authentication.

- 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.

New York State

- New York State Information Technology Standard Number: NYS-S13-003, Sanitization/Secure Standard.
  - Available at: https://its.ny.gov/document/sanitizationsecure-disposal-standard.
- New York State Information Technology Standard Number: NYS-S14-002, Information Classification Standard.
  - Available at: https://its.ny.gov/document/information-classification-standard.

SUNY

- SUNY Policy Document Number: 6609, Records Retention and Disposition.
  - Available at: https://www.suny.edu/sunypp/documents.cfm?doc_id=650.

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 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