ACCESS CONTROL POLICY

policy.fredonia.edu

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-103*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

This Access Control Policy establishes an Access Control Program for managing risks through user account management, access enforcement and monitoring, separation of duties and roles, and remote access. The State University of New York at Fredonia (*"Fredonia"*) Access Control Policy serves to be consistent with best practices associated with organizational Information Security management. This policy establishes access control protocols throughout Fredonia and its Business Units to implement security best practices surrounding logical security, account management, and remote access.

This Policy is based on the Access Control principles established in NIST SP 800-53 "Access Control," Control Family guidelines. 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 Access Control Policy process helps Fredonia to ensure that only the appropriate people have access to the Information Assets, Business Systems, and Information Technology Resources that they are authorized to have access to, and ensures protections to eliminate unauthorized access to the systems and resources. The Access Control Program helps Fredonia implement security practices that require logical security, account management, and remote access to the system and resources.

II. POLICY STATEMENT

It is the Policy of Fredonia to establish Access Controls to manage risks through user account management, access enforcement and monitoring, separation of duties and roles, and remote access protocols. Each Fredonia Functional/Business unit utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources must adhere to the access controls outlined in this Policy, and must develop or adhere to a program plan that demonstrates compliance with the standards enumerated in this Policy.

This policy is applicable to all Information Technology (IT) 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 email, messages and files) is the property of Fredonia. All users of IT resources, including Fredonia employees, students, affiliates, contractors, vendors or similar, are responsible for adhering to this policy.

ACCESS CONTROL POLICY

All Fredonia Functional/Business Units must take action to implement the Access Control steps outlined in the NIST SP 800-53 "Access Control," Control 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. Access Control Policy and Procedures: (AC-1):
   Fredonia System Custodian(s):
   a) Develops, documents, and disseminates to all users of IT resources that utilize University regulated data and/or systems:
      1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
   b) Reviews and updates the current:
      1. Access control policy annually; and
      2. Access control procedures as needed.
2. Account Management: (AC-2)[1]:
   Fredonia System Owners employ automated mechanisms to support the management of information system accounts.
3. Access Enforcement: (AC-3)[1]:
   The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
4. Information Flow Enforcement: (AC-4)[1]:
   The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on Fredonia Information Security Data Access Policy and Data Access Standard.
5. Separation of Duties: (AC-5)[1]:
   Fredonia System Owners:
   a) Separates system administration, programming, configuration management, quality assurance and testing, security auditing, network security, and technical support in accordance with staffing and funding limitations;
   b) Documents separation of duties of individuals; and
   c) Defines information system access authorizations to support separation of duties.
6. Least Privilege: (AC-6)[1]:
   Fredonia System Owners employs the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
7. Unsuccessful Login Attempts: (AC-7)[1]:

The information system:

a) Enforces a limit on unsuccessful login attempts by locking the account.

b) Automatically unlocks the account after a preset time period or until released by an administrator.

8. System Use Notification: (AC-8):

The information system:

a. Displays to users the System/Network Login Banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

> "W A R N I N G - This computer system is the property of the State University of New York at Fredonia. It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with the University's Acceptable Use Policy ("AUP"). The full policy can be found at: https://tinyurl.com/acceptable-use-policy-pdf
> -The University complies with state and federal law regarding certain legally protected confidential information, but makes no representation that any uses of this system will be private or confidential. Users should have no expectation of personal privacy in any materials they place, view, access, or transmit on this system.
> -Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions as set forth in the University's AUP.
> -By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.
> If you do not agree to the conditions stated in this warning, then please DO NOT log in."

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c.For publicly accessible systems:

1. Per the Systems and Network Banner Login Banner noted above.

9. Session Lock: (AC-11)[1]:

The information system:

a. Prevents further access to the system by initiating a session lock after a minimum of 3 hours of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

10. Session Termination: (AC-12)[1]:

The information system automatically terminates a user session after 30 days.

11. Permitted Actions w/o identification or Authentication: AC(-14)[1]:

Fredonia System Owners:

a. Identifies organization-defined user actions and ISO approved business need that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

12. Remote Access: (AC-17)[1]:

Fredonia System Owners:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections.

13. Wireless Access: (AC-18)[1]:

Fredonia System Owners:

a.Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b.Authorizes wireless access to the information system prior to allowing such connections.

14. Access Control for Mobile Devices: (AC-19)[1]:

Fredonia System Owners:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b. Authorizes the connection of mobile devices to organizational information systems.

15. Use of External Information Systems: (AC-20)[1]:

Fredonia System Owners establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and

b. Process, store, or transmit organization-controlled information using external information systems.

16. Information Sharing: AC(-21)[1]:

Fredonia System Owners:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved third party information systems; and

b.Employs the Data Risk Classification Policy (See Data Examples) to assist users in making information sharing/collaboration decisions.

17. Publicly Accessible Content: (AC-22)[1]:

Fredonia System Owners:

a. Designates individuals authorized to post information onto a publicly accessible information system;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d. Reviews the content on the publicly accessible information system for nonpublic information on an on-going basis and removes such information, if discovered.

[1] Note: This 800-53 security control directly relates to CUI security requirement 3.1 Access Control 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 800-46 Rev 2
  - Special Publication 800-46 Rev 2, Guide to Enterprise Telework and Remote Access Security, United States Department of Commerce National Institute for Standards and Technology (NIST), June 2009.
- NIST 800-113
  - Special Publication 800-113, Guide to SSL VPNs, United States Department of Commerce National Institute for Standards and Technology (NIST), July 2008.
- NIST 800-114 Rev 1
  - Special Publication 800-114 Rev 1, User's Guide to Securing External Devices for Telework and Remote Access, United States Department of Commerce National Institute for Standards and Technology (NIST), November 2007.
- NIST 800-121 Rev 2
  - Special Publication 800-121 Rev 2, Guide to Bluetooth Security, United States Department of Commerce National Institute for Standards and Technology (NIST), October 2016.
- NIST 800-48 Rev 1
  - Special Publication 800-48 Rev 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, United States Department of Commerce National Institute for Standards and Technology (NIST), July 2008.
- 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), February 2007.
- NIST 800-97
  - Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, United States Department of Commerce National Institute for Standards and Technology (NIST), February 2007.
- NIST 800-124
  - Special Publication 800-124, Guidelines on Cell Phone and PDA Security, United States Department of Commerce National Institute for Standards and Technology (NIST), June 2013.
- NIST 800-77
  - Special Publication 800-77, Guide to IPsec VPNs, United States Department of Commerce National Institute for Standards and Technology (NIST), December 2005.
- 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-S14-013, Account Management/Access Control Standard.
  - Available at: https://its.ny.gov/document/account-management-access-control-standard
- New York State Information Technology Standard Number: NYS-S14-010, Remote Access Standard Access Control Standard.
  - Available at: https://its.ny.gov/document/remote-access-standard

IV. DEFINITIONS

TERM	DEFINITION
Business Systems	Any and all Information Technology (IT) resources and information assets owned and/or operated by Fredonia.
System Custodian	A System Custodian is an employee of the University or Affiliate who has administrative and/or operational responsibility over a system that utilizes Category II - Private or Category III - Restricted University data. A system may include software (e.g. application) hosted on-campus or off-campus (e.g. cloud). In many cases, there will be multiple System Custodian. An enterprise application may have teams of Data Custodians, each responsible for varying functions. System Custodian is responsible for the following: ● Understanding and reporting on how Fredonia's data is stored, processed and transmitted by their system. ● Working with the Fredonia Information Security Office, implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of Fredonia's regulated data. ● Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of Fredonia's data. ● Provisioning and deprovisioning access to Fredonia's data as authorized by the Data Steward, Trustee, or Owner. ● System Custodians are responsible for provisioning and deprovisioning access based on criteria established by the appropriate Data Steward.

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 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