IDENTIFICATION & AUTHENTICATION POLICY

policy.fredonia.edu

Effective Date	*1/29/2020*
Policy Number	*TEC-PL-107*
Sponsor	*Chief Information Officer (CIO)*
Responsible Office	*Information Technology Services (ITS)*
Next Review Date	*1/29/2024*

I. REASON FOR POLICY

This Identification and Authentication Policy establishes a process for managing risks from user access (organizational, non-organizational) and authentication into State University of New York at Fredonia (*"Fredonia"*) information assets through the establishment of an effective identification and authentication program.

The Fredonia Identification and Authentication Policy serves to be consistent with best practices associated with organizational Information Security management. This Policy establishes the requirement of an identification and authentication management process throughout Fredonia and its Functional/Business Units. The identification and authentication program helps Fredonia implement security best practices with regard to identification and authentication into Fredonia information assets.

Each Fredonia Functional/Business 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 Identification and Authentication principles established in NIST SP 800-53 "Identification and Authentication Family guidelines."

An adequate Identification and Authentication process helps Fredonia manage the risks of improper access to Fredonia system assets, will aid in the proper management and monitoring of such assets, and is key component relating to information system audit processes. This Policy establishes the requirement of an identification and authentication process throughout Fredonia and its Functional/Business Units to help the organization ensure that the organization adheres to industry best practices regarding identification and authentication into Fredonia 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 Identification and Authentication process that ensures security best practices and capabilities throughout Fredonia and its Functional/Business Units. The purpose of an Identification and Authentication process is to help manage the risks associated with inappropriate use or unauthorized access to all information systems. Unauthorized access, or authorized access for inappropriate purposes, may intentionally or unintentionally render Fredonia systems unsecure and make retention of required audit evidence difficult or impossible. Proper identification and authentication is critical for ensuring that Fredonia systems have not been compromised. Each Fredonia Functional/Business Units utilizing Fredonia Information Assets, Business Systems, and Information Technology Resources must adhere to the identification and authentication 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. Identification and Authentication Policy and Procedures: (IA-1):
   Fredonia:
   - a. Develops, documents, and disseminates to Fredonia employees and Affiliates that utilize University regulated data and/or systems:
     1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
     2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
   - b. Reviews and updates the current:
     1. Identification and authentication policy annually; and
     2. Identification and authentication procedures as needed.
2. Identification and Authentication (Organizational Users) : (CM-2: 2.1, 2.2, 2.3, 2.8, 2.9)[1]:
   The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
   Network Access To Privileged Accounts (2.1): The information system implements multifactor authentication for network access to privileged accounts
   Network Access To Non-privileged Accounts (2.2): The information system implements multifactor authentication for network access to non privileged accounts.

Local Access To Privileged Accounts (2.3): The information system implements multifactor authentication for local access to privileged accounts.
Network Access To Privileged Accounts - Replay Resistant (2.8): The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.
Network Access To Non-privileged Accounts - Replay Resistant (2.9): The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

3. Device Identification: (IA-3):
   The information system uniquely identifies and authenticates the user through a dedicated user account (e.g. eServices account) before establishing a local, remote, or network connection.
4. Identifier Management: (IA-4)[1]:
   Fredonia manages information system identifiers by:
   a. Receiving authorization from an authoritative source or sponsor (e.g. Human Resources, Deans Office, Vice President Office, Admissions etc.) to assign an individual, group, role, or device identifier;
   b. Selecting an identifier (e.g. Fredonia I.D. or Visitor I.D.) that identifies an individual, group, role, or device;
   c. Assigning the identifier to the intended individual, group, role, or device;
   d. Preventing reuse of identifiers; and
   e. Disabling the identifier after the individual, group, role, or device is no longer officially affiliated with Fredonia.
5. Authenticator Management: (IA-5: 5.1)[1]:
   Fredoniamanages information system authenticators by:
   a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
   b. Establishing initial authenticator content for authenticators defined by the organization;
   c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
   d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
   e. Changing default content of authenticators prior to information system installation;
   f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
   g. Changing/refreshing authenticators as needed;
   h. Protecting authenticator content from unauthorized disclosure and modification;
   i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
   j. Changing authenticators for group/role accounts when membership to those accounts changes.

Password-based Authentication (5.1): The information system, for password-based authentication:

(a) Enforces minimum password complexity of the following:

- Not contain the user's account name or parts of the user's full legal name that exceed two consecutive characters
- Be at least 10 characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)

(b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];

(c) Stores and transmits only cryptographically-protected passwords;

(d) Enforces password minimum and maximum lifetime restrictions if appropriate;

(e) Prohibits password reuse for 24 generations; and

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

6. Authenticator Feedback: (IA-6)[1]:

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

7. Cryptographic Module Authentication: (IA-7):

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

8. Identification and Authentication (Non-Organizational Users): (IA-8):

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

9. Service Identification and Authentication: (IA-9):

Fredonia identifies and authenticates the users using current industry standard security safeguards.

10. Adaptive Identification and Authentication: (IA-10):

Fredonia requires that individuals accessing the information system employ current industry standard supplemental authentication techniques or mechanisms under specific circumstances or situations.

11. Re-authentication: (IA-11):

Fredonia requires users and devices to re-authenticate when the account has been inactive for a maximum of 30 minutes for Category III - Restricted data access and 3 hours for Category II - Private or Category I - Public data access and/or on each new session created.

[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

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 800-100
  - 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 800-78-4
  - Special Publication 800-78-4 Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV), United States Department of Commerce National Institute for Standards and Technology (NIST), May 2015.
    - Summary: This document contains the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201-2 as well as the supporting infrastructure specified in FIPS 201-2 and the related NIST Special Publication 800-73-4, Interfaces for Personal Identity verification [SP800-73], and NIST SP 800-76-2, Biometric Specifications for Personal Identity Verification [SP800-76], that rely on cryptographic functions.

- 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 800-73-4
  - Special Publication 800-73-4 Interfaces for Personal Identity Verification, United States Department of Commerce National Institute for Standards and Technology (NIST), August 2016.
    - Summary: This document contains the technical specifications to interface with the smart card to retrieve and use the PIV identity credentials. The specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, card edge interface, and application programming interface. Moreover, this document enumerates requirements where the international integrated circuit card standards [ISO7816] include options and branches.

  - 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

New York State

- New York State Information Technology Standard Number: NYS-S14-008, Secure Configuration Standard.
  - Available at: https://its.ny.gov/document/secure-configuration-standard

- New York State Information Technology Standard Number: NYS-S14-007, Encryption Standard.
  - Available at: https://its.ny.gov/document/encryption-standard

- New York State Information Technology Standard Number: NYS-P10-006, Identity Assurance Policy.
  - Available at: https://its.ny.gov/document/identity-assurance-Policy

- New York State Information Technology Standard Number: NYS-S13-004, Identity Assurance Standard.
  - Available at: https://its.ny.gov/document/identity-assurance-standard

- New York State Information Technology Standard Number: NYS-S13-004, Authentication Tokens Standard.
  - Available at: https://its.ny.gov/document/authentication-tokens-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 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