IDENTIFICATION AND AUTHENTICATION STANDARD

Standard Title:	**IDENTIFICATION AND AUTHENTICATION STANDARD**
Standard Number:	**38-10.7**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**IDENTIFICATION AND AUTHENTICATION (IA)**
Approval Date:	**07/19/2024**
Responsible Office:	**Office of Information Technology**
Responsible Executive:	**Chief Information Officer**

Applies to: All employees, students, visitors, and contractors, in all academic and operational departments and offices at all Norfolk State University locations, and to all university information technology and data, whether owned and operated by the university, or used for university business through contractual arrangements.

STANDARD STATEMENT

All individuals to whom this standard applies shall comply with the Norfolk State University Information Security Standards and protect all IT systems and data to which they have access commensurate with sensitivity and risk. All university information technology and data whether owned and operated by the university or used for university business through contractual arrangements shall be managed and protected in accordance with the provisions of the Norfolk State University Information Security Standards.

TABLE OF CONTENTS PAGE NUMBER

STANDARD STATEMENT 1
DEFINITIONS 1
CONTACT(S) 3
STAKEHOLDER(S) 3
IDENTIFICATION AND AUTHENTICATION (IA) 4
EDUCATION AND COMPLIANCE 7
EXCEPTIONS 7
REVIEW SCHEDULE 7
RELATED DOCUMENTS 7

DEFINITIONS

Authorization: The process of verifying that a requested action or service is approved for a specific entity.

Authorize: A decision to grant access, typically automated by evaluating a subject's attributes.

Authorized: A system entity or actor that has been granted the right, permission, or capability to access a system resource.

Availability: The property that data or information is accessible and usable upon demand by an authorized person and that timely, reliable access to data and information services is provided for authorized users.

Computer Network: Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Confidentiality: Protection of systems and data so that unauthorized parties cannot view the data, the property that sensitive information is not disclosed to unauthorized entities, and the assurance that information is not disclosed to unauthorized individuals or processes.

Controlled Unclassified Information (CUI): Information the Federal government owns or has created that needs to be safeguarded and disseminated using only controls consistent with Federal laws, regulations and policies.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An individual, who defines, manages, and controls the use of data and ensures compliance with the Information Security Standards with respect to the data.

Information Security: The policies, standards, guidelines, processes, activities, and actions taken to protect the confidentiality, integrity, and availability of information systems and the data they handle commensurate with sensitivity and risk.

Information Security Incident: means an adverse event or situation, whether intentional or accidental, that poses an enterprise impact or threat to the integrity, availability, or confidentiality of university data or systems or requires reporting based upon regulatory requirements.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control.

Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Intellectual Property: Please refer to the BOV POLICY # 35 (2019) INTELLECTUAL PROPERTY POLICY.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

Sensitive Information/Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

System Administrator: An individual or entity that implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An individual or entity responsible for the operation and maintenance of an IT system.

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the University which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, and computer furnishings operated or maintained by NSU.

Users: Faculty, staff and students as well as others who have been authorized to use Norfolk State University's technological resources, (e.g., contractors, interns, volunteers, etc.).

CONTACT(S)

The Office of Information Technology (OIT) officially interprets this standard. OIT is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Questions regarding this standard should be directed to OIT Security.

STAKEHOLDER(S)

University Faculty & Staff
Students
Others who have been authorized to use Norfolk State University's technological resources.

IDENTIFICATION AND AUTHENTICATION (NSU-IA)

NSU-IA-1 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control:

a. Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users;

b. Implement multi-factor authentication for access to privileged accounts;

c. When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources;

d. Implement multi-factor authentication for remote access to privileged accounts and non-privileged accounts such that:

   1. One of the factors is provided by a device separate from the system gaining access; and

   2. The device meets organization-defined strength of mechanism requirements;

e. Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts; and

f. Provide a single sign-on capability for organization-defined system accounts and services.

NSU-IA-2 IDENTIFIER MANAGEMENT

Control: Manage system identifiers by:

a. Receiving authorization from a designated organizational official to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device;

d. Preventing reuse of identifiers for at least one year; and

e. Maintain the attributes for each uniquely identified individual, device, or service in organization-defined protected central storage.

NSU-IA-3 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued 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 or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators at least every 180 days for user accounts and 42 days for administrator accounts;

g. Employ multi-factor authentication for all users;

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific controls to protect authenticators;

j. Changing authenticators for group or role accounts when membership to those accounts changes;

k. For password-based authentication:

   a. Transmit passwords only over cryptographically-protected channels;

   b. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

   c. Require immediate selection of a new password upon account recovery;

   d. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

   e. Enforce the following composition and complexity rules;

   f. Password authenticators must:

      i. Be at least 14 characters in length;

      ii. Utilize each of the following four:

         1. Special characters (e.g. !@#$%&);

         2. Numerical characters;

         3. Upper case letters; and

         4. Lower case letters; and

      iii. Prohibits password reuse for 24 generations; and

l. Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation;

m. Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage;

n. Prohibit the reuse of authenticators when accounts are used across multiple individual systems;

o. For biometric-based authentication, employ mechanisms that satisfy best practice biometric quality requirements;

p. Prohibit the use of cached authenticators after 180 days for users and 42 days for administrator accounts;

q. For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications;

r. Require that the issuance of organization-defined types of and/or specific authenticators be conducted in person or by a trusted external party before organization-defined registration authority with authorization by organization-defined personnel or roles;

s. Employ organization-defined password managers to generate and manage passwords; and

t. Protect the passwords using organization-defined controls.

NSU-IA-4

Control: The organization manages information system authenticators for users and devices by:

a. Requiring passwords with a minimum of 6 characters on smart phones or PDAs accessing or containing NSU data;

b. Requiring passwords to be set on device management user interfaces for all network-connected devices;

NSU-IA-5 AUTHENTICATOR FEEDBACK

Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

NSU-IA-6 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

NSU-IA-7 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control:

a. Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users; and

b. Conform to the profiles for identity management as described in the account naming convention.

NSU-IA-8 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: Uniquely identify and authenticate system services and applications before establishing communications with devices, users, or other services or applications.

NSU-IA-9 RE-AUTHENTICATION

Control: Require users to re-authenticate when organization-defined circumstances or situations requiring re-authentication.

NSU-IA-10 IDENTITY PROOFING

Control:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual;

c. Collect, validate, and verify identity evidence;

d. Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization; and

e. Require evidence of individual identification be presented to the registration authority.

IDENTIFICATION AND AUTHENTICATION STANDARD

EDUCATION AND COMPLIANCE

This standard shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

- Communicate the standard in writing, electronic or otherwise, to the University community within 30 days of approval;
- Post the standard on the appropriate Website; and
- Educate and train all stakeholders and appropriate audiences on the standard's content, as necessary. Failure to meet the publication requirements does not invalidate this standard.

The Chief Information Security Officer (or designee) is responsible for official interpretation of this standard. Questions regarding the application of this standard should be directed to the Office of Information Technology. The Chief Information Security Officer reserves the right to revise or eliminate this standard.

Violations of this standard, including without limitation any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to comply with requirements of this standard may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may violate federal, state, or local laws.

EXCEPTIONS

Exceptions to this standard must be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Information Officer, and the Chief Information Security Officer.

REVIEW SCHEDULE

- Next Scheduled Review: **07/19/2026**
- Approval by, date: OIT Standards Development Group, **07/19/2024**
- Revision History: 7/31/2025
- Supersedes: SEC530 IA Controls

RELATED DOCUMENTS

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx
32-02 - Data Classification Policy

https://www.nsu.edu/policy/admin-32-02.aspx

38-10 - Information Security Policy

https://www.nsu.edu/policy/bov-38-10.aspx