UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38-05 (2021) Identification and Authentication Policy

Policy Title:	Identification and Authentication Policy
Policy Type:	Board of Visitors
Policy Number:	BOV #38-05 (2021)
Approval Date:	May 14, 2021
Responsible Office:	Office of Information Technology (OIT)
Responsible Executive:	Vice President for Operations and Chief Strategist for Institutional Effectiveness
Applies to:	All Norfolk State University (NSU) employees (classified, hourly, official representatives, and third-party vendors)

POLICY STATEMENT

The Identification and Authentication policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of identification and authentication controls at Norfolk State University. This includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, identification and authentication best practices, and the requirements defined in this policy. Positively identifying potential network users, hosts, applications, services, and permitting or denying access to resources will provide protection of, and mitigate risks to, NSU's information systems, data, and users.

This policy also meets the control requirements outlined in Commonwealth of Virginia Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC-501, Section 8.7 Identification and Authentication Family which includes specific requirements for the Commonwealth of Virginia.

Table of Contents **Page Number**

DEFINITIONS

Authentication: The process of verifying the identity of a user to determine the right to access specific types of data or IT systems.

Chief Information Officer (CIO): Oversees the operation of NSU Information Technologies. Responsible for policies, procedures, and standards for assessing security risks, determining the appropriate security measures and performing security audits.

Client Services: Branch within the Office of Information Technology that provides support to faculty, staff, and currently enrolled students to resolve IT related issues and requests concerning on campus computer systems and equipment.

Cryptography: The process of transforming plain text into cipher text, and cipher text into plain text.

Director of IT Security (DIS): The senior management designated by the CIO of NSU to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of information systems and data.

Encryption: The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users.

Two-factor authentication/Multifactor Authentication: The utilization of two of the factors (something you know: a password or personal identification number (PIN); something you have: a token, such as bank card; something you are: biometrics, such as fingerprints and voice recognition.) to verify a user's identity. Multi-factor authentication (MFA) could involve two of the factors or it could involve all three.

Identification: The process of associating a user with a unique user ID or login ID.

Office of Information Technology (OIT): The Office of Information Technology manages the administrative and academic information technology resources for Norfolk State University.

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38-05 (2021) Identification and Authentication Policy

System Owner: An NSU Manager designated by the Agency Head or Information Security Officer, who is responsible for the operation and maintenance of an agency IT system.

System Administrator: An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner.

CONTACT(S)

The Office of Information Technology officially interprets this policy. The Chief Information Officer is responsible for obtaining approval for any revisions as required by BOV Policy #1 (2014) Creating and Maintaining Policies through the appropriate governance structures. Questions regarding this policy should be directed to the Office of Information Technology, (757) 823-2916.

STAKEHOLDER(S)

All University Faculty, Staff, Students, & Community.

IDENTIFICATION AND AUTHENTICATION POLICY

OIT will develop, disseminate, review and update the Identification and Authentication Policy on an annual basis to preserve the confidentiality, integrity, and availability of NSU's information systems and data.

A. IDENTIFICATION AND AUTHENTICATION

1. Administrators of the information system shall ensure that the information system:

    a. Uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Organizational users include organizational employees or individuals NSU deems to have equivalent status of employees. The Administrator will assign user identifiers to ensure that no two users have the same identifier.

    b. Implements multifactor authentication for network access to privileged accounts. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection.

2. Administrators of the information system shall:

    a. Require individuals to be authenticated with an individual authenticator when a group authenticator is employed.

b. Ensure that network connections for accessing development environments or performing administrative functions on servers or multi-user systems employ two-factor authentication and are audited. Two-Factor authentication is required for all network-based administrative access to servers and multi-use systems.

B. IDENTIFIER MANAGEMENT

1. Administrators of the information system shall manage information system identifiers by:

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

    b. Selecting an identifier 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 for at least 24 changes of the identifier and at least 24 days from the initial use of the identifier.

    e. Disabling the identifier after 90-days of inactivity.

C. AUTHENTICATOR MANAGEMENT

1. System Owners shall require administrators of the information system to manage 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. Default content of authenticators (i.e., passwords provided for initial entry to a system) must be changed by the Administrator before implementation of the information system or component.

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.

g. Changing/refreshing user-account authenticators at least every 90-days.

h. Changing/refreshing administrative authenticators at least every 42-days.

i. Protecting authenticator content from unauthorized disclosure and modification.

j. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.

i. All Supervisors shall ensure their users protect authenticators by:

1. Maintaining exclusive control and use of their passwords by not loaning or sharing authenticators with others.

2. Protecting them from inadvertent disclosure to others.

3. Posting or displaying passwords is prohibited.

4. Reporting lost or compromised authenticators immediately.

ii. Devices must be configured to safeguard authenticators (e.g., certificates).

2. Administrators of the information system shall ensure, for password-based authentication, that the information system:

a. Enforces minimum password complexity of:

i. At least eight characters in length.

ii. At least three of the following four:

1. Special characters.

2. Alphabetical characters.

3. Numerical characters.

4. Combination of upper case and lower case letters.

b. Stores and transmits only encrypted representations of passwords.

c. Enforces password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum or dual factor authentication. Unless authorized by the System Owner, passwords cannot be changed in less than one (1) day.

d. Prohibits password reuse for 24 generations. Password history must be set so a user cannot quickly reuse a previous password.

e. Allows the use of a temporary password for system logons with an immediate change to a permanent password. Passwords (other than initial) must be chosen by users, not assigned by administrators or help desk staff.

f. Changing/refreshing sensitive system authenticators at least every 42-days.

3. The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

4. The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

5. The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

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

a. Requiring passwords with a minimum of four characters on smart phones or PDAs accessing or containing COV data.

b. Requiring that forgotten initial passwords be replaced rather than reissued.

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

d. Documenting and storing hardware passwords securely.

e. Requiring passwords not be cached or stored on the device.

f. Requiring the suppression of passwords on the display as the password is entered into the device.

7. An organization sponsoring an Internet-facing system containing sensitive data provided by private citizens, which is accessed by only those citizens providing the stored data shall:

   a. Determine the appropriate validity period of the password, commensurate with sensitivity and risk.

   b. Determine the appropriate number of passwords to be maintained in the password history file, commensurate with sensitivity and risk.

   c. Allow the citizen to continue to use the initial password so long as the Agency provides a mechanism to the citizen that allows the citizen to create a unique initial password.

   d. The account holder must be provided with information on the importance of changing the account password on a regular and frequent basis.

D. Authenticator Feedback

1. The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals (e.g., masked upon entry by displaying asterisks or dots when a user types in a password, not displaying it in clear text).

E. Cryptographic Module Authentication

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

F. Identification and Authentication (Non-NSU Users)

1. The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Non-organizational users include all information system users other than organizational users already explicitly covered.

EDUCATION AND COMPLIANCE

A. SECURITY POLICY TRAINING

Security policy training is intended to educate NSU employees who have a role in IT system security and to help foster an understanding of how NSU security policies protect the University employees, students, systems, and data.

1. NSU employees, who manage, administer, operate, or design IT systems, must receive role-based security training that is commensurate with their role.

2. As necessary, OIT will educate and train all stakeholders and appropriate audiences on the policy's content using virtual or face-to-face engagements.

B. POLICY COMPLIANCE AND VIOLATIONS

1. OIT measures compliance with information security policies and standards through processes that include, but are not limited to monitoring and audits.

2. Violations of this policy will be addressed in accordance with relevant NSU and Commonwealth of Virginia policies, including NSU Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual basis by the appropriate executive or designee.

PUBLICATION

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

1. Communicate the policy in writing, electronic or otherwise, to the NSU community within 14 days of approval.
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval.

3. Educate and train all stakeholders and appropriate audiences on the policy's content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: May 2024
- Approval by, date: May 14, 2021
- Revision History: *New Policy*
- Supersedes policies: *New Policy*

RELATED DOCUMENTS

1. ADMINISTRATIVE POLICY # 32-01 (2014) Acceptable Use of Technological Resources: https://www.nsu.edu/policy/admin-32-01.aspx.

2. ITRM Information Security Policy (SEC519): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

3. ITRM Information Security Standard (SEC501): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

4. Virginia Department of Human Resources Management Policy 1.75: http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf?sfvrsn=2