ACCESS CONTROL STANDARD (NSU-AC)

Standard Title:	**ACCESS CONTROL STANDARD (NSU-AC)**
Standard Number:	**38-10.1**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**ACCESS CONTROL (AC)**
Approval Date:	**10/21/2024**
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

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.

ACCESS CONTROL (AC)

NSU-AC-1 ACCOUNT MANAGEMENT

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require organization-defined prerequisites and criteria for group and role membership;
d. Specify:
    1. Authorized users of the system;
    2. Group and role membership; and
    3. Access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Require approvals by designated personnel for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with the University-defined logical access control policy or standard;
g. Monitor the use of accounts;
h. Notify OIT within:
    1. One business day when accounts are no longer required;
    2. One business day of when users are terminated or transferred; and
    3. One business day when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;
j. With the exception of permissions granted per the Information Security Access Agreement (ISAA), review accounts for compliance with account management requirements on an annual basis and following an environmental change;
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group;
l. Align account management processes with personnel termination and transfer processes;
m. Support the management of system accounts using organization-defined automated mechanisms;
n. Automatically disable temporary and emergency accounts after no more than 30 days;
o. Disable accounts within one business day of notification when the accounts:
    1. Have expired;
    2. Are no longer associated with a user or individual;
    3. Are in violation of organizational policy; or

4. Have been inactive for 90 days; and

p. Automatically audit account creation, modification, enabling, disabling, and removal actions.
q. Establish and administer privileged user accounts in accordance with a role-based access scheme;
r. Monitor privileged role or attribute assignments;
s. Monitor changes to roles or attributes; and
t. Revoke access when privileged role or attribute assignments are no longer appropriate.
u. Monitor system accounts for atypical or suspicious usage; and
v. Report atypical usage of system accounts to the Chief Information Security Officer or designee

NSU-AC-2 NSU-AC-2

Control: NSU shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

a. For all internal and external IT systems:
    1. Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.
    2. Disable unneeded accounts in a timely manner.
    3. Retain unneeded accounts in a disabled state in accordance with the records retention policy.
    4. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.
    5. Require that the System Administrator and the Chief Information Security Officer or designee investigate any unusual system access activities.
    6. Require the System and Data Owner approve changes to access level authorizations.
    7. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
    8. Prohibit the granting of local administrator rights to users. The Chief Information Security Officer or designee may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exceptions must be documented annually and include the Chief Information Security Officer or designee's explicit acceptance of residual risks.
    9. Require that at least two individuals have administrative accounts to each IT system.
    10. The information system automatically audits account creation, disabling, and termination actions and notifies, as required, appropriate individuals.

11. Temporarily disable logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.
12. Disable logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

b. For all internal IT systems:
   1. Require a documented request from the user to establish an account on any internal IT system.
   2. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.
   3. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner and Data Owner or designees to establish accounts for all sensitive IT systems.
   4. Require secure delivery of access credentials to the user based on information already on file.
   5. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.
   6. Promptly remove access when no longer required.

c. For all external IT systems, require secure delivery of access credentials to users of all external IT systems.

d. For all service and hardware accounts:
   1. Document account management practices for all University created service accounts, including, but not limited to granting, administering and terminating accounts. If the service or hardware account is not used for interactive login with the system, the service or hardware account is exempt from the requirement to change the password at the interval defined in the standard containing password or authenticator management requirements.
   2. If the IT system is classified as sensitive, prohibit the use of guest accounts.
   3. If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:
      (a) Are documented according to standard practice and maintained on file;
      (b) Include access attributes for the account;
      (c) Are approved by the System Owner and communicated to the CISO; and
      (d) Expire after a predetermined period, based on sensitivity and risk.

NSU-AC-3 ACCESS ENFORCEMENT

a. Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control standards.
b. Enforce a role-based access control policy over defined subjects and objects and control access based upon organization-defined roles and users authorized to assume such roles.
c. Release information outside of the system only if:
    1. The receiving organization authorized system or system component provides security controls that meet University security standards; and
    2. The organization-defined controls are used to validate the appropriateness of the information designated for release.

NSU-AC-4 INFORMATION FLOW ENFORCEMENT

a. Enforces approved authorizations for controlling the flow of information within the system and between connected systems based on the appropriate organization-defined information policies and standards.

NSU-AC-5 SEPARATION OF DUTIES

a. Identify and document separation of duties of individuals; and
b. Define system access authorizations to support separation of duties.

NSU-AC-6 LEAST PRIVILEGE

a. Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
b. Authorize access for organization-defined individuals or roles to:
    1. Organization-defined security functions (deployed in hardware, software, and firmware); and
    2. Organization-defined security-relevant information.
c. Require that users of system accounts (or roles) with access to organization-defined security functions or security-relevant information use non-privileged accounts or roles, when accessing nonsecurity functions.
d. Restrict privileged accounts on the system to administrative personnel.
e. Prohibit privileged access to the system by non-organizational users or individuals not under the contractual control of the University.
f. Review on an annual basis the privileges assigned to sensitive system users to validate the need for such privileges; and
g. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.
h. Log the execution of privileged functions.
i. Prevent non-privileged users from executing privileged functions.

NSU-AC-7 UNSUCCESSFUL LOGON ATTEMPTS

a. Enforce a limit of 5 consecutive invalid logon attempts by a user during a 15 minute period; and
b. Automatically locks the account or node for a minimum of a 30 minute period or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
c. Purge or wipe information from mobile devices based on organization-defined purging or wiping requirements and techniques after 10 consecutive, unsuccessful device logon attempts.
d. Limit the number of unsuccessful biometric logon attempts to 5 where possible.
e. Allow the use of organization-defined authentication factors that are different from the primary authentication factors after the number of organization- defined consecutive invalid logon attempts have been exceeded; and
f. Enforce a limit of 5 consecutive invalid logon attempts through use of the alternative factors by a user during a 15 minute period.

NSU-AC-8 SYSTEM USE NOTIFICATION

a. Display organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and states that:
    1. Users are accessing a system;
    2. System usage may be monitored, recorded, and subject to audit;
    3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
    4. Use of the system indicates consent to monitoring and recording;
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 system; and
c. For publicly accessible systems:
    1. Display system use information, before granting further access to the publicly accessible system;
    2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
    3. Include a description of the authorized uses of the system.

NSU-AC-9 CONCURRENT SESSION CONTROL

a. Limit the number of concurrent sessions for each server and database administrative account to 5.

NSU-AC-10 DEVICE LOCK

a. Prevent further access to the system by initiating a device lock after 15 minutes of inactivity or upon receiving a request from a user; and
b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.
c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

NSU-AC-11 SESSION TERMINATION

a. Automatically terminate a user session after 24 hours.
b. Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to information resources.
c. Display an explicit logout message to users indicating the termination of authenticated communications sessions.

NSU-AC-12 REMOTE ACCESS

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorize remote access to the system prior to allowing such connections.
c. Employ automated mechanisms to monitor and control remote access methods.
d. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
e. Route all remote accesses through authorized and managed network access control points.
f. Protect information about remote access mechanisms from unauthorized use and disclosure.
g. Provide the capability to disconnect or disable remote access to the system within 15 minutes.

NSU-AC-13 NSU-AC-13

a. When connected to internal networks guest networks or non-University networks, data transmission shall only use full tunneling and not use split tunneling.
b. Protect the security of remote file transfer of sensitive data to and from IT systems by means of approved encryption.
c. Require that IT system users obtain formal authorization and a unique user ID and password prior to using remote access capabilities.
d. Document requirements for the physical and logical hardening of remote access devices.
e. Require maintenance of auditable records of all remote access.
f. Where supported by features of the system, session timeouts shall be implemented after a period of no longer than 15 minutes of inactivity and less, commensurate with sensitivity

and risk. Where not supported by features of the system, mitigating controls must be implemented.

g. The organization ensures that remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.

NSU-AC-14 WIRELESS ACCESS

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections.
c. Protect wireless access to the system using authentication based on user or device and encryption.
d. Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.
e. Identify and explicitly authorize users allowed to configure wireless networking capabilities.

NSU-AC-15 NSU-AC-15

a. The Chief Information Security Officer is accountable for ensuring the following steps are followed and documented:
b. Wireless LAN (WLAN) Connectivity on the University Networks
    1. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal network.
        (a) LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;
        (b) All WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;
c. WLAN Hotspot (Wireless Internet)
    1. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:
        (a) WLAN Hotspots must have logical or physical separation from the agency's LAN;
        (b) WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;
        (c) All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and
d. Wireless Bridging
    1. The following network configuration shall be used when bridging two wired LANs:
        (a) All wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption methods

(i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);

(b) Wireless bridging devices will not have a default gateway configured;

(c) Wireless bridging devices must be physically or logically separated from other networks;

(d) Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network; and

(e) Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

NSU-AC-16 ACCESS CONTROL FOR MOBILE DEVICES

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
b. Authorize the connection of mobile devices to organizational systems.
c. Employ either full-device encryption or container encryption to protect the confidentiality and integrity of information on mobile devices.

NSU-AC-17 USE OF EXTERNAL SYSTEMS

a. Establish terms and conditions, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
    1. Access the system from external systems; and
    2. Process, store, or transmit organization-controlled information using external systems.
b. Prohibit the use of unapproved external systems.
c. Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:
    1. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
    2. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.
d. Restricts the use of organization-controlled portable storage devices by authorized individuals on non-University information systems.
e. Restrict the use of non-approved systems or system components to process, store, or transmit organizational information.

NSU-AC-18 INFORMATION SHARING

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for organization-defined information sharing circumstances where user discretion is required.

NSU-AC-19 PUBLICLY ACCESSIBLE CONTENT

a. Designate individuals authorized to make information publicly accessible;
b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
d. Review the content on the publicly accessible system for nonpublic information prior to initial posting, quarterly, and remove such information, if discovered.

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: 10/21/2026

- Approval by, date: OIT Standards Development Group, 10/21/2025
- Revision History: 4/10/2025,10/23/2025
- Supersedes: SEC530 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