UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38-02 (2020) Logical Access Control Policy

Policy Title:	Logical Access Control Policy
Policy Type:	Board of Visitors
Policy Number:	BOV #38-02 (2020)
Approval Date:	December 11, 2020
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 Logical Access Control policy identifies the security controls defined to enforce logical access control measures for information technology (IT) systems, programs, processes, and information. The policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with the responsibility to implement access controls. This policy establishes the requirements for the Logical Access Controls.

This policy also meets the control requirements outlined in Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC-501, Section 8.1 Access Control Family, Controls AC-1 through AC-16, AC-22, to include specific requirements for COV in AC-2-COV and AC-8-COV.

TABLE OF CONTENTS **PAGE NUMBER**

DEFINITIONS

Access Controls: A set of security procedures that monitor access and either allow or prohibit users from accessing information systems and data. The purpose of access controls is to prevent unauthorized access to information systems.

Authentication: The process of verifying an 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.

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

Guest/Anonymous/Temporary Account: A default set of permissions and privileges given to non-registered users of a system or service.

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 (OIT) manages the administrative and academic information technology resources for Norfolk State University.

System Owner: A 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 NSU Faculty, Staff, Students, & Community.

LOGICAL ACCESS CONTROL POLICY

In accordance with SEC501, AC-1 through AC-16 and AC-22, to include specific requirements for Commonwealth of Virginia (COV) in AC-2-COV and AC-8-COV, OIT will develop, disseminate, and update the Logical Access Controls Policy on at least an annual basis. System Owners shall control and document the logical access control of information systems and their respective components.

A. Account Management

1. All NSU directorates will ensure proper access management of NSU-owned systems and systems belonging to business partners who house NSU-owned information.
2. The System Owner shall create an Access Control Document that defines the processes and procedures that staff will use to manage access to IT systems. The document will include, at a minimum, the following:
    a. An account type dictionary which includes a list of all account types used by NSU system (i.e., individual, group, system, service, application, guest/anonymous, temporary, etc.) and a definition of that account type.
    b. A group membership policy definition section which establishes a list of all groups, conditions for group membership, and the process for reissuing group account credentials when a user is removed from a group. For example, group membership includes but is not limited to access grouped by Read Only or Read/Write.
    c. A well-defined process for identifying an authorized user's access to the information system and for specifying access privileges and other attributes. The process will include:
        - Definition of required approvals for requests to establish new accounts.
        - Definition of required approvals for requesting modification (addition or subtraction of privileges).
        - Process for establishing, activating, modifying, disabling, and removing accounts.
        - Procedures for specifically authorizing and monitoring the use of guest/anonymous and temporary accounts.
    d. A process for notifying account managers when temporary accounts are no longer required and when information system users are terminated or transferred, or when information system usage or need-to-know/need-to-share changes.
3. The System Owner shall review accounts and privileges at least quarterly at a minimum.

4. The user's supervisor and the System Owner (or designee) shall approve all user access to NSU systems.
    a. As part of the access request, the user's supervisor must provide the user's need for access.
    b. The System Owner (or designee) will maintain the documented approvals.
    c. The DIS or designee, shall approve accounts for users requiring administrative and/or privileged access.
5. The DIS and the System Owner will ensure that no local administrator rights are granted unless there is a documented exception on file for employees that are primarily responsible for developing and/or supporting IT applications and infrastructure.
6. A user's supervisor must notify Human Resources, the System Owner and OIT using the online Clearance Form when a user's account is no longer required. User access must be disabled within 24 hours of notification.
    a. Logical access rights must be temporarily disabled when:
        - Personnel do not need system access for a prolonged (period over 30 days) because they are not working due to leave, disability or other authorized purposes.
        - Personnel are suspended more than 1 day for disciplinary purposes.
7. The System Owner or designee must monitor account usage to ensure that no account goes over 90 consecutive days without usage.
    a. The information system must be configured to automatically disable accounts when not used for 90 days.
8. The System Owner or designee shall approve emergency access to sensitive IT systems for a predetermined period not to exceed 30 days, and notify the CIO for oversight. If the emergency access request leads to changes in the user's access level, attributes for the account are included in the documentation and maintained on file.
    a. The information system must be configured to automatically terminate temporary and emergency accounts after the predetermined period or 30 days, whichever comes first.
9. The System Owner or designee must keep on file, all user account data, information, and documentation associated with a user's logical access, in accordance with NSU policy.
10. The System Owner shall be responsible for ensuring that:

a. At least two individuals have administrative accounts for each IT system in order to help provide continuity of operations.

b. System Administrators have both an administrative account and at least one user account and that administrators use their administrative accounts only when performing tasking requiring administrative privileges.

c. Account deactivation occurs:

- When temporary accounts are no longer required
- Within 24 hours of notification of user termination or transfer

d. Disabled accounts are retained in accordance with NSU's records retention policy.

e. Activation of accounts or granting of privileges (access) requires:

- The principles of least privilege
- Valid access authorization documentation
- Intended system usage
- Meeting NSU missions and business functions
- The Human Resources policy that a background check must be completed before (or as soon as feasible after) establishment of a user account

f. Users are not sharing accounts unless the system resides on a guest network.

g. Access credentials, for internal IT systems, must be delivered to the user in a confidential manner based on information already on file.

h. Access credentials, for Internet-facing only systems (i.e. public websites) must be securely delivered (e.g., by alternate channels such as U.S. Mail) to external users that request access to any sensitive external IT system.

i. The information system automatically audits account creation, modification, and disabling, as well as termination actions and notifies, as required, appropriate individuals.

j. Access levels are associated with group membership where practical, and every system user account is a member of at least one user group.

k. Guest accounts are prohibited on sensitive IT systems.

l. All service and hardware accounts are documented, including, but not limited to granting, administering and terminating access.

- If the service or hardware account is not used for interactive login with the system, the account is exempt from the requirement to change the password at the interval defined in the Identification and Authentication Policy.

m. In cases where two-factor authentication cannot be used, the analysis of why two-factor authentication is not used must be documented.

11. Users of IT systems shall ensure that:
    a. Accounts are not being shared.
    b. Initial passwords are changed upon first use.
    c. Proper notification is given to System Owners to temporarily disable access when the user will not need such access for a prolonged period (over 30 days) due to leave, disability or other authorized purposes.
    d. System use is within the policies and guidelines.
12. System Owners and System Administrators must investigate any unusual system access activities observed in logs or reported to them by staff and employees. Investigation activities shall include the following:
    a. Monitor for atypical or suspicious usage of information system accounts.
    b. Report atypical usage to the DIS.
    c. Track and monitor privileged role assignments (e.g., key management, network and system administration, database administration, and web administration).
    d. Disable accounts posing a significant risk to the IT system.
13. A contractor's continued need for access to all IT systems must be reviewed at least annually:
    a. System Owners will advise contractors of the need to recertify a continued need for access to the system.
    b. The contractor will advise the supervisor by email of the need to recertify.
    c. The supervisor will review the need and notify the System Owner of the continued need.

B. Access Enforcement

1. System Owners must employ and document access control mechanisms. These include but are not limited to identity-based policies, role-based policies, attribute-based policies, and access enforcement mechanisms such as access control lists, access control matrices, and cryptography.

C. Information Flow Enforcement

1. System Owners must ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with the applicable policy.
   a. Flow control restrictions include, but are not limited to, the following:
      - Keeping data export controlled information from being transmitted in the clear to the Internet.
      - Blocking outside traffic that claims to be from within NSU.
      - Not passing any web requests to the Internet that are not from the internal user networks, an authorized server or web proxy.
   b. Flow control is based on the characteristics of the information and/or the information path.

      Note: Flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using keyword searches or document characteristics).

D. Separation of Duties

1. The System Owner separates the duties of individuals as necessary, to prevent malevolent activity without collusion.
2. The System Owner is responsible for ensuring and documenting the separation of duties.
3. The System Owner, in coordination with the systems administrator, will implement separation of duties through assigned information system access authorizations.
4. Separation of duties include, but are not limited to, the following:
   a. Mission functions and distinct information system support functions are divided among different individuals/roles.
   b. Different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security).
   c. Security personnel who administer access control functions do not administer audit functions.

d. Different administrator accounts for different roles.

E. Least Privilege

1. NSU shall employ the concept of Least Privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with NSU missions and business functions.
   a. The System Owner is responsible for ensuring that each user has only enough access to conduct their job.
   b. The DIS, or designee, explicitly approves and authorizes access to administrative or privileged accounts.
      - Super-user accounts will be limited to system administration personnel.
   c. The System Owner requires that users of information system accounts, or roles that access administrative accounts use non-privileged accounts, or roles, when accessing other system functions, and if feasible, system owner shall audit any use of privileged accounts, or roles, for such functions.
   d. The System Owner prohibits privileged access to the information system by non-NSU users unless employed specifically to provide support for the system (e.g. Vendor support for such a system).

F. Unsuccessful Login Attempts

1. OIT and the System Owner will implement a policy for unsuccessful logins. The policy shall be documented in the OIT access control document and enforced automatically by the system.
   a. The information system will be configured to:
      - Enforce a limit of a maximum of 3 consecutive attempts within 15 minutes.
      - Automatically lock a non-sensitive account/node for a minimum period of 15 minutes when the maximum number of unsuccessful attempts is exceeded.
      - Automatically lock a sensitive account until released by an administrator when the maximum number of unsuccessful attempts is exceeded.
   b. These controls apply regardless of whether the login occurs via a local or network connection. However, an organization may opt for more stringent controls on remote connections if practical.
   c. The information system provides additional protection for mobile devices, such as smartphones or personal digital assistants, accessed via login by purging

information from the device after ten consecutive, unsuccessful login attempts to the device.

- This requirement may not apply to mobile devices if the information on the device is encrypted with sufficiently strong encryption mechanisms thus making purging unnecessary.
- The login is to the mobile device, not to any one account on the device. Consequently, a successful login to any account on the mobile device resets the unsuccessful login count to zero.

G. System Use Notification

1. The System Owner must notify users, both internal and external to NSU, that the monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the CIO); and user commands; email and Internet usage; message and data content.
   a. The information system must be configured to:
      - Display an approved system use notification message or banner that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance, before granting access to the system. Guidance must state that:
        1. Users are accessing a Norfolk State University information 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.
        4. The use of the system indicates consent to monitoring and recording.
      - Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information system.
   b. Publicly accessible systems will:
      - Display the system use information when appropriate, before granting further access.
      - Display references, if any, to monitoring, recording, or auditing that is consistent with private accommodations for such systems that generally prohibit those activities.

- Include in the notice given to public users of the information system, a description of the authorized uses of the system.

H. Session Lock

1. The System Owner is responsible for implementing a session locking policy that prevents further access to the system by initiating a session lock after a maximum of 30 minutes, or less, of inactivity or upon receiving a request from a user.
   a. The user should log off of systems not currently being used.
2. The System Owner is responsible to ensure that a session lock is retained until the user reestablishes access using established identification and authentication procedures.

I. Session Termination

1. The system owners must address the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for a local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system.
2. The information system sessions must automatically terminate a user session after 24 hours of inactivity.

J. Permitted Action Without Identification or Authentication

1. It is the policy of NSU to ensure that all system users be identified and authenticated to ensure proper access to the system. However, from time to time it may become necessary for a system to grant access without authentication. In these cases, the following must be adhered to:
   a. The System Owner is responsible for identifying and documenting specific user actions that can be performed without identification or authentication.
      - Documentation and the supporting rationale must be included in the System Security Plan.
   b. The System Owner is responsible for providing limited access to specific functions based on a particular need to accomplish a particular business or mission.

K. Use of External Information Systems

1. OIT must establish 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.

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

2. System Owners and the DIS must ensure security control enhancements for sensitive systems are implemented in accordance with SEC501 Section AC-20 Section 1-4.

L. Publicly Accessible Content

1. The System Owner shall designate individuals authorized to post information to an NSU information system that is publicly accessible.
2. The System Owner is responsible for training authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
3. The System Owner or designee reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the NSU information system.
4. The System Owner or designee reviews the content on the publicly accessible NSU information system for nonpublic information at least every 60-days.
5. The System Owner (or designee) removes nonpublic information from the publicly accessible NSU information system if discovered.

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:

- Communicate the policy in writing, electronic or otherwise, to the NSU community within 14 days of approval;
- Submit the policy for inclusion in the online Policy Library within 14 days of approval;
- 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: December 2023
- Approval by, date: December 11, 2020
- 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