UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #38-08 (2022) Remote, Wireless, and Mobile Access Policy

Policy Title:	Remote, Wireless, and Mobile Access Policy
Policy Type:	Board of Visitors
Policy Number:	BOV #38-08 (2022)
Approval Date:	April 13, 2022
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 Remote, Wireless, and Mobile Access policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of remote, wireless, and mobile access security controls at Norfolk State University. This policy includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, remote, wireless, and mobile access best practices, and the requirements defined in this policy. The Remote, Wireless, and Mobile Access Control policy, establishes usage restrictions, configuration requirements, connection requirements, implementation guidance and direction for the use of remote access capabilities, and the implementation of wireless technologies. The increasing use of remote connections, wireless networking, and dissemination of mobile devices places Norfolk State University at greater risk. This policy is intended to minimize potential exposure and limit remote, wireless, and mobile access security concerns.

This policy meets the control requirements outlined in Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC501, Section 8.1 Access Control Family, Controls AC-17 through AC-20, to include specific requirements for COV in AC-17-COV and AC-20-COV.

Table of Contents **Page Number**

POLICY STATEMENT 1
DEFINITIONS 2
STAKEHOLDER(S) 3
REMOTE, WIRELESS, AND MOBILE ACCESS POLICY 4
EDUCATION AND COMPLIANCE 9
PUBLICATION 9

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #38-08 (2022) Remote, Wireless, and Mobile Access Policy

REVIEW SCHEDULE 10

RELATED DOCUMENTS 10

DEFINITIONS

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

Configure: To set the functional and physical characteristics of an item.

Cryptography: A method of protecting information and communications by transforming plain text into cipher text and cipher text into plain text so that only those for whom the information is intended can read and process it.

Default Gateway: A routing device or hardware node that passes outgoing and incoming traffic between the different subnet and network destinations.

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 unauthorized users cannot read it.

Full-Device Encryption: A cryptographic method that applies encryption to an entire hard drive including data, files, the operating system, and software programs.

Hotspots: A specific location that provides Internet access via a wireless local area network (WLAN); generally synonymous with a Wi-Fi connection.

Information Security Officer (ISO): The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's information security program.

Malicious Activity: Harmful code introduced into a program or file to contaminate, damage, or destroying information systems and/or data. Malicious activity includes viruses, Trojan horses, trap doors, worms, spyware, and counterfeit computer instructions (executables).

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

Remote Access: The ability to get access to a computer or a network from a remote distance.

Sensitive Data: Any data of which the compromise, with respect to confidentiality, integrity, and/or availability, could adversely affect NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled.

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.

Two-Factor 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 a bank card; something you are: biometrics, such as fingerprints and voice recognition.) to verify a user's identity.

Technological Resources (TR): 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.

Wireless Bridging: A wireless bridge is a networking hardware device that connects two wired networks over Wi-Fi. The wireless bridge acts as a client, logging in to the primary router and getting an Internet connection. It passes on to the devices connected to its local area network (LAN) segments, bridging a wireless connection between them.

Wireless Local Area Network (WLAN): A wireless computer network that links two or more devices using wireless communication. WLANs use high-frequency radio waves and often include an access point to the Internet. A WLAN allows users to move around the coverage area while maintaining a network connection.

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

REMOTE, WIRELESS, AND MOBILE ACCESS POLICY

OIT will review and update the Remote, Wireless, and Mobile Access policy on an annual basis or more frequently if required to address changes.

A. REMOTE ACCESS

1. The Director of IT Security (DIS) or designee shall:

    a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

    b. Authorize remote access to the information system before allowing such connections.

2. The DIS or designee shall ensure the information system:

    a. Monitors and controls remote access methods.

    b. Implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

    c. Routes all remote accesses through managed network access control points.

3. The DIS or designee shall:

    a. Authorize the execution of privileged commands and access to security-relevant information via remote access only for organization-defined needs.

    b. Document the rationale for such access in the security plan for the information.

    c. Ensure that users protect information about remote access mechanisms from unauthorized use and disclosure.

    d. Provide the capability to expeditiously disconnect or disable remote access to the information system within sixty (60) minutes.

    e. Ensure only full tunneling and not split tunneling is used for data transmission when connected to internal networks from COV guest networks or non-COV networks.

f. Protect the security of remote file transfer of sensitive data to and from agency IT systems using approved encryption.

g. Require that IT system users obtain formal authorization and unique user identification and password prior to using the Agency's remote access capabilities.

h. Document requirements for the physical and logical hardening of remote access devices.

i. Require maintenance of auditable records of all remote access.

j. Implement session timeouts after a period of no longer than 30 minutes of inactivity or less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.

k. Ensure that remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.

B. **WIRELESS ACCESS**

1. The Director of IT Security (DIS) or designee shall:

   a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

   b. Authorize wireless access to the information system prior to allowing such connections.

2. The Director of IT Security (DIS) or designee shall ensure the information system protects wireless access to the system using authentication and encryption.

3. The System Owner or designee shall disable wireless networking capabilities internally embedded within information system components prior to issuance and deployment when not intended for use.

4. The Chief Information Officer (CIO) or designee shall:

   a. Identify and explicitly authorize users allowed to configure wireless networking capabilities independently.

b. Select radio antennas and calibrate transmission power levels to reduce the probability of receiving usable signals outside of organization-controlled boundaries.

5. The Information Security Officer (ISO) or designee shall ensure the DIS or designee documents and follows requirements concerning the deployment, configuration, and administration of Wireless Local Area Network (WLAN) infrastructure connected to any internal COV network, such as the following:

    a. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates).

    b. WLAN infrastructure must authenticate each client device prior to permitting access to the WLAN.

    c. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources.

    d. Only COV owned or leased equipment shall be granted access to an internal WLAN.

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

    f. Physical or logical separation between WLAN and wired LAN segments must exist.

    g. All COV WLAN access and traffic must be monitored for malicious activity and associated event log files stored on a centralized storage device.

    h. WLAN clients will only permit infrastructure mode communication.

6. The Information Security Officer (ISO) or designee shall ensure the DIS or designee documents and follows the following when building a wireless network that will only provide unauthenticated access to the Internet:

    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.

d. WLAN clients only permit infrastructure mode communication where COV clients are concerned.

7. The Information Security Officer (ISO) or designee shall ensure the DIS or designee documents and follows the following network configuration 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.

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

C. ACCESS CONTROL FOR MOBILE DEVICES

1. The DIS or designee shall:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

b. Authorize the connection of mobile devices to organizational information systems.

c. Employ either full-device encryption or container encryption to protect the confidentiality and integrity of information on mobile devices.

D. USE OF EXTERNAL INFORMATION SYSTEMS

1. The Information Security Officer (ISO) or designee shall:

   a. Establish terms and conditions consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems when authorizing individuals to:

      i. Access the information system from external information systems.

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

   b. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

      i. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

      ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

   c. Restrict the use of organization-controlled portable storage devices by authorized individuals on external information systems.

   d. Prohibit the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information.

   e. Prohibit the use of network-accessible storage devices in external information systems.

   f. Identify whether personal IT assets are allowed onto premises that house IT systems and data and if so, identify the controls necessary to protect these IT systems and data.

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 commensurate with their role. Personnel with assigned security roles and responsibilities will be trained:

    a. Before authorizing access to the information system or performing assigned duties.

    b. When required by information system changes.

    c. As practical and necessary thereafter.

2. 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, Acceptable Use of Technological Resources, and Department of Human Resources Management Policy 1.75, Use of Electronic Communications and Social Media. 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: April 13, 2025
- Approval by, date: April 13, 2022
- Revision History: *New Policy*
- Supersedes policies: *New Policy*

RELATED DOCUMENTS

1. ADMINISTRATIVE POLICY # 32- 01 (2021) 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. ITRM Information Security Standard (SEC514): https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

5. Virginia Department of Human Resources Management Policy 1.75, Use of Electronic Communications and Social Media: https://hr.dmas.virginia.gov/media/1243/dhrm-policy-175-use-of-electronics-and-social-media.pdf

6. Library of Virginia Personnel Records General Schedule (GS)-103 (Feb 2015): https://www.lva.virginia.gov/agencies/records/sched_state/GS-103.pdf