UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV #38-04 (2021) Security Awareness and Training Policy

Policy Title:	Security Awareness and Training Policy
Policy Type:	Board of Visitors
Policy Number:	BOV #38-04 (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 Security Awareness and Training policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of security awareness and training controls at Norfolk State University. This includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, security awareness and training best practices, and the requirements defined in this policy. Raising awareness and informing NSU community members of their obligations will strengthen the University's understanding of Information Technology (IT) security threats, risks, and roles. Security awareness is a shared responsibility and a continuous process that reinforces expectations of behavior, actions, and activities critical to protecting the confidentiality, integrity, and availability of systems and data utilized by the University.

This policy meets the control requirements outlined in Commonwealth of Virginia Information Technology Resource Management (ITRM) Information Security Policy SEC519 and Security Standard SEC501, Section 8.2 Security Awareness and Training Family, Controls AT-1 through AT-4, to include specific requirements for the Commonwealth of Virginia.

Table of Contents **Page Number**

Policy Statement 1
Definitions 2
Stakeholder(s) 3
Security Awareness and Training Policy 3
Education and Compliance 5
Publication 6
Review Schedule 6
Related Documents 6

DEFINITIONS

Acceptable Use Policy (AUP): A document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet.

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.

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.

Intellectual property: An invention from the human intellect that is protected for the creator's use under the law as a patent, copyright, trademark, or trade secret.

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 Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying information systems and/or data. Malicious code includes viruses, Trojan horses, trap doors, worms, spy-ware, 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.

Phishing: A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

Privacy: The rights and desires of an individual to limit the disclosure of individual information to others.

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

Security Awareness: A critical part of incident prevention, particularly when it comes to social engineering threats used to manipulate individuals into giving away private information.

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.

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for information systems and data.

Social Engineering: A critical part of incident prevention, particularly when it comes to social engineering threats used to manipulate individuals into giving away private information.

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.

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

SECURITY AWARENESS AND TRAINING POLICY

OIT will review and update the Security Awareness and Training policy on an annual basis or more frequently if required to address changes.

A. SECURITY AWARENESS

1. The Director of IT Security (DIS) or designee shall provide basic security awareness training to system users (including managers, senior executives, and contractors):

    a. As part of initial training for new users.

b. When required due to system changes.

c. Annually or more often as necessary thereafter.

2. The DIS or designee shall include practical exercises in security awareness training that simulate actual cyber-attacks.

3. The DIS or designee shall include security awareness training on recognizing and reporting potential indicators of insider threat.

4. The DIS or designee shall develop an information security training program so that each system user is aware of and understands the following concepts:

   a. NSU's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data.

   b. The concept of separation of duties.

   c. Prevention and detection of information security incidents, including those caused by malicious code.

   d. Proper disposal of data storage media.

   e. Proper use of encryption.

   f. Access controls, including creating and changing passwords and the need to keep them confidential.

   g. NSU's policy for acceptable use.

   h. NSU's policy for Remote Access.

   i. Intellectual property rights, including software licensing and copyright issues.

   j. Responsibility for the security of COV data.

   k. Phishing.

   l. Social engineering.

   m. Least privilege.

5. The DIS or designee shall require documentation of IT system user's acceptance of NSU's security policies after receiving information security training.

    a. Each manager is responsible for ensuring that their respective employees complete mandatory Security Awareness Training.

    b. The DIS or designee may revoke account access until mandatory Security Awareness Training is completed.

6. The Agency Head must receive role-based training as related to the requirements of the commonwealth's information security program as defined in SEC501 Section 2.4.

B. ROLE-BASED SECURITY TRAINING

1. The DIS or designee shall provide role-based security training to personnel with assigned security roles and responsibilities:

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

    b. When required due to system changes.

    c. As practical and necessary thereafter.

C. SECURITY TRAINING RECORDS

1. The DIS or designee shall:

    a. Document and monitor individual system security training activities including basic security awareness training and specific information system security training.

    b. Retain individual training records for three (3) years in accordance with the Library of Virginia retention schedule.

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. 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: http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf?sfvrsn=2

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