UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #10 (2023) Security Assessment and Authorization Policy

Policy Title:	Security Assessment and Authorization Policy
Policy Type:	Board of Visitors
Policy Number:	BOV UISP #10 (2023)
Approval Date:	December 8, 2023
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 Assessment and Authorization policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of security assessment and authorization controls at Norfolk State University. This policy includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, security assessment and authorization best practices, and the requirements defined in this policy. The Security Assessment and Authorization policy facilitates the assurance that applicable technical and non-technical security controls are in place, known vulnerabilities/threats have been identified and mitigated, and systems are operating as intended. It is vital to understand and explicitly accept the risk that a system could pose to the overall University. Additionally, it will enable NSU to maintain security of systems over time in a highly dynamic environment, particularly when resources are limited, and the University must prioritize its efforts.

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 SEC501, Section 8.4 Security Assessment and Authorization Family, Controls CA-1, CA-3, CA-3-COV, CA-6, CA-7, CA-8.

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #10 (2023) Security Assessment and Authorization Policy

Table of Contents **Page Number**

DEFINITIONS

Agency Head: Responsible for the security of the University's information technology resources and data. Designates the Information Security Officer (ISO) and System Owners.

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.

Data Owner: An agency manager responsible for decisions regarding data, such as evaluating and classifying data, defining and communicating protection requirements for data, identifying legal or regulatory requirements and business needs, and defining access requirements.

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

Interconnection Security Agreements (ISA): A documented agreement that defines security-relevant technical requirements between any two directly connected systems, owned and operated under two different distinct authorities, for the purpose of sharing data and other information resources.

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 policies and program.

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #10 (2023) Security Assessment and Authorization Policy

Information Technology (IT): 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, data files and/or documents managed or maintained by the University which reside on disk, tape or other media.

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

Penetration Testing: The technique of evaluating the security posture of a system or network by simulating the hacking methods of a malicious attacker.

Sensitive 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.

System Owner: An agency manager is responsible for the overall procurement, training, development, integration, modification, operation, maintenance, retirement, and risk and compliance of an information system.

CONTACT(S)

The Office of Information Technology (OIT) 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

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #10 (2023) Security Assessment and Authorization Policy

SECURITY ASSESSMENT AND AUTHORIZATION POLICY

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

A. INFORMATION SYSTEM CONNECTIONS (ISA)

1. The System Owner(s) or designee(s) shall:

    a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements (ISA). This applies to dedicated connections between information systems, and does not apply to transitory, user-controlled connections such as email and website browsing.
    b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated. Instead of developing an ISA, this information may be incorporated into a formal contract, especially if the connection is to be established between NSU and a non-Commonwealth (i.e., private sector) organization.
    c. Review and update, if necessary, ISA's annually or more frequently if required to address an environmental change.

2. For every sensitive NSU IT system that shares data with non-Commonwealth entities, the DIS or designee shall require or shall specify that its service provider require:

    a. System Owners, in consultation with the Data Owner, to document IT systems with which data is shared. This documentation must include:

        i. The types of shared data.
        ii. The direction(s) of data flow.
        iii. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.

    b. System Owners of interconnected systems must:

        i. Inform one another of connections with other systems.
        ii. Notify each other prior to establishing connections to other systems.

c. A written agreement specifying:

i. If and how the shared data will be stored on each IT system.
ii. System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., FERPA) regarding handling, protecting, and disclosing of the shared data.
iii. Each Data Owner's authority to approve access to the shared data.

d. System Owners approve and enforce the agreement.

B. SECURITY AUTHORIZATION

1. The Agency Head or designee shall:

a. Assign a senior-level executive or manager as the authorizing official for the information system.
b. Ensure that the authorizing official authorizes the information system for processing before commencing operations. If the connecting systems have the same Authorizing Official, an ISA is not required. However, if the connecting systems have different Authorizing Officials but the Authorizing Officials are in the same organization, ISO shall determine whether an ISA is required.
c. Update, if necessary, security authorizations on an annual basis or more frequently if required to address an environmental change.

C. CONTINUOUS MONITORING

1. The DIS or designee shall develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

a. Establishment of metrics to be monitored.
b. Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring.
c. Ongoing security control assessments.
d. Ongoing security status monitoring of metrics.
e. Correlation and analysis of security-related information generated by assessments and monitoring.
f. Response actions to address results of the analysis of security-related information.
g. Reporting the security status of the organization and the information system to appropriate organizational officials at least every 120 days.

D. **PENETRATION TESTING**

1. The CIO or designee shall conduct penetration testing on an annual basis or more frequently if required to address an environmental change on any system housing commonwealth 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 IT 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.

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #10 (2023) Security Assessment and Authorization Policy

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: December 8, 2026
- Approval by, date: December 8, 2023
- 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