UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #38-07 (2022) Risk Assessment Policy

Policy Title:	Risk Assessment Policy
Policy Type:	Board of Visitors
Policy Number:	BOV #38-07 (2022)
Approval Date:	December 9, 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 Risk Assessment Policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of risk assessment controls at Norfolk State University. This policy includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, risk assessment best practices, and the requirements defined in this policy. The Risk Assessment Policy provides a foundation for identifying risk, assessing risk, and the steps to take to reduce risk to an acceptable level within IT systems. Risk Assessments account for information technology (IT) threats, vulnerabilities, likelihoods, and impact to operations and assets, individuals, and other partnering organizations, based on the use of NSU's information systems. Effective implementation of risk management is a critical component of a successful IT security program. Therefore, NSU must exercise due care and diligence in the implementation and operation of IT systems.

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 8.14 Risk Assessment Family, Controls RA-1, RA-2, RA-3, RA-5.

Table of Contents **Page Number**

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #38-07 (2022) Risk Assessment Policy

DEFINITIONS

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): 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.

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.

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.

Platform Enumeration: A naming scheme for describing and identifying classes of information technology systems, such as applications, operating systems, and hardware devices present among an organization's computing assets.

Risk: A function of the likelihood of a given threat source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization. Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence.

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #38-07 (2022) Risk Assessment Policy

Risk Assessment: The process of identifying and evaluating risks to assess their potential impact. A review, examination, and judgment of whether or not the identified risks are acceptable.

System Owner: An agency manager 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.

STAKEHOLDER(S)

All NSU Faculty, Staff, Students, & Community

RISK ASSESSMENT POLICY

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

A. SECURITY CATEGORIAZATION

1. The ISO or designee shall:

    a. Categorize information and the information system in accordance with applicable Commonwealth laws, Executive Orders, directives, policies, regulations, standards, and guidance.

    b. Document the security categorization results in the security plan for the information system.

    c. Ensure that the security categorization decision is reviewed and approved by the authorizing official or authorized official designated representative.

B. RISK ASSESSMENT

1. The ISO or designee shall:

    a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

    b. Document risk assessment results in a Risk Assessment Report.

    c. Review risk assessment results annually or more frequently if required to address an environmental change.

    d. Disseminate risk assessment results to the appropriate organization-defined personnel.

    e. Update the risk assessment on an annual basis or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the state of the security system.

C. VULNERABILITY SCANNING

1. The DIS or designee shall:

    a. Scan for vulnerabilities in the information system and host applications at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported.

    b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

        i. Enumerating platforms, software flaws, and improper configurations.

        ii. Formatting checklists and test procedures.

        iii. Measuring vulnerability impact.

c. Analyze vulnerability scan reports and results from security control assessments.

d. Remediate legitimate vulnerabilities within 90-days in accordance with an organizational assessment of risk.

e. Share information obtained from the vulnerability scanning process and security control assessments with the appropriate organization-defined personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

f. Employ vulnerability scanning tools that can readily update the information system vulnerabilities to be scanned.

g. Update the information system vulnerabilities scanned at least once every 90-days.

h. Employ vulnerability scanning procedures to identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

i. Determine what information about the information system is discoverable by adversaries and take appropriate corrective actions.

j. Review historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

2. The System Owner or designee shall ensure that the information system implements privileged access authorization to information system components for selected vulnerability scanning activities.

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. Therefore, 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 policy 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.

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 9, 2025
- Approval by, date: December 9, 2022

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #38-07 (2022) Risk Assessment Policy

- 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, 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