UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #11 (2023) System and Information Integrity Policy

Policy Title:	System and Information Integrity Policy
Policy Type:	Board of Visitors
Policy Number:	BOV UISP #11 (2023)
Approval Date:	December 8, 2023
Responsible Office:	Office of Information Technology (OIT)
Responsible Executive:	Vice President for Operations and Institutional Effectiveness
Applies to:	All Norfolk State University (NSU) employees (classified, hourly, official representatives, and third-party vendors)

POLICY STATEMENT

The System and Information Integrity policy addresses the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance required to establish an acceptable level of system and information integrity controls at Norfolk State University. This includes, but is not limited to, any regulatory requirements that Norfolk State University is subject to, system and information integrity best practices, and the requirements defined in this policy. The System and Information Integrity policy ensures that NSU's Information Technology (IT) resources and information systems are instituted with system integrity monitoring in mind. It covers areas of concern such as malware, application and source code flaws, industry supplied alerts, and remediation of detected or disclosed integrity issues.

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 8.17 System and Information Integrity Family, Controls SI-1, SI-2, SI-2-COV, SI-3, SI-3-COV, SI-4, SI-5-COV, SI-8, SI-9, and SI-10.

Table of Contents **Page Number**

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #11 (2023) System and Information Integrity Policy

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.

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.

Input Validation: Checking the type and content of data supplied by a user or application (i.e., input validation, for web applications, means verifying user inputs provided in web forms, query parameters, and uploads). malicious code

Malicious Code/Program: Harmful code 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): OIT manages the administrative and academic information technology resources for Norfolk State University.

Spam: Unsolicited and unwanted junk email sent out in bulk to an indiscriminate recipient list. Typically, spam is sent for commercial purposes. It can be sent in massive volume by networks of infected computers.

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.

UNIVERSITY INFORMATION SECURITY POLICY (UISP)
BOV UISP #11 (2023) System and Information Integrity Policy

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

SYSTEM AND INFORMATION INTEGRITY POLICY

OIT will review and update the System and Information Integrity policy on an annual basis or more frequently if required to address changes.

A. **FLAW REMEDIATION**

1. The System Administrator or designee shall:

    a. Identify, report, and correct information system flaws.
    b. Investigate software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
    c. Install publisher security-relevant software and firmware updates as soon as possible after appropriate testing, not to exceed 90 days of the release date of the updates.
    d. Incorporate flaw remediation into organizational change management.

2. The CIO or designee shall:

    a. Prohibit the use of software products that the software publisher has designated as End-of- Life/End-of-Support (i.e., software publisher no longer provides security patches for the software product).

B. **MALICIOUS CODE PROTECTION**

1. The DIS or designee shall:

    a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
    b. Update malicious code protection mechanisms whenever new releases are available in accordance with organizational change management policy.

c. Configure malicious code protection mechanisms to:

   i. Perform periodic scans of the information system and real-time scans of files from external sources at network entry/exit points as well as the destination host as the files are downloaded, opened, or executed.
   ii. Quarantine malicious code; send alert to administrator in response to malicious code detection.

d. Address false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
e. Centrally manage malicious code protection mechanisms.

2. The DIS or designee shall ensure that the information system automatically updates malicious code protection mechanisms.

3. The CIO or designee shall:

   a. Prohibit:

      i. Malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, trojan horses, etc.).
      ii. Users from propagating malicious programs including opening attachments from unknown sources.

4. The Agency Head or designee shall prohibit the use of software on the University's network until the software is approved by the CIO or designee where practicable.

5. The DIS or designee shall:

   a. Provide protection against malicious programs through the use of mechanisms that:

      i. Eliminate or quarantines malicious programs that it detects.
      ii. Provide an alert notification.
      iii. Periodically run scans on memory and storage devices.
      iv. Scan all files retrieved through a network connection, modem connection, or from an input storage device.
      v. Allow only authorized personnel to modify program settings.
      vi. Maintain a log of protection activities.

b. Provide:

   i. The ability for download of definition files for malicious code protection programs whenever new files become available and propagates the new files to all devices protected by the malicious code protection program.
   ii. Instruction to administrators and IT system users on how to respond to malicious program attacks, including shut-down, restoration, notification, and reporting requirements.
   iii. Network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.
   iv. Malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

c. Require all forms of malicious code protection start automatically upon system boot.
d. Establishes Operating System (OS) update schedules commensurate with sensitivity and risk.

C. INFORMATION SYSTEM MONITORING

1. The DIS or designee shall:

   a. Monitor the information system to detect:

      i. Attacks and indicators of potential attacks.
      ii. Unauthorized local, network, and remote connections.

   b. Identify unauthorized use of the information system.
   c. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

2. The DIS or designee shall ensure that the information system monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

3. The DIS or designee shall:

   a. Analyze communications traffic/event patterns for the information system.
   b. Develop profiles representing common traffic patterns and/or events.
   c. Use the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.

4. The DIS or designee shall employ:

    a. A wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches.

    b. An intrusion detection system to monitor wireless communications traffic.

5. The DIS or designee shall correlate information from employed monitoring tools.

D. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

1. The DIS or designee shall:

    a. Receive information system security alerts, advisories, and directives from the appropriate external organizations on an ongoing basis.
    b. Generate internal security alerts, advisories, and directives as deemed necessary.
    c. Disseminate security alerts, advisories, and directives.
    d. Implement security directives.

E. SPAM PROTECTION

1. The DIS or designee shall:

    a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
    b. Update spam protection mechanisms when new releases are available.

F. INFORMATION INPUT VALIDATION

1. The System Administrator or designee shall ensure that:

    a. The information system checks the validity of information inputs.

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.

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 (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-policy175-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