SYSTEM & INFORMATION INTEGRITY STANDARD

Standard Title:	**SYSTEM & INFORMATION INTEGRITY STANDARD (NSU-SI)**
Standard Number:	**38-10.18**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**SYSTEM AND INFORMATION INTEGRITY (SI)**
Approval Date:	**10/21/2024**
Responsible Office:	**Office of Information Technology**
Responsible Executive:	**Chief Information Officer**

Applies to: All employees, students, visitors, and contractors, in all academic and operational departments and offices at all Norfolk State University locations, and to all university information technology and data, whether owned and operated by the university, or used for university business through contractual arrangements.

STANDARD STATEMENT

All individuals to whom this standard applies shall comply with the Norfolk State University Information Security Standards and protect all IT systems and data to which they have access commensurate with sensitivity and risk. All university information technology and data whether owned and operated by the university, or used for university business through contractual arrangements shall be managed and protected in accordance with the provisions of the Norfolk State University Information Security Standards.

TABLE OF CONTENTS PAGE NUMBER

DEFINITIONS

Authorization: The process of verifying that a requested action or service is approved for a specific entity.

Authorize: A decision to grant access, typically automated by evaluating a subject's attributes.

Authorized: A system entity or actor that has been granted the right, permission, or capability to access a system resource.

Availability: The property that data or information is accessible and usable upon demand by an authorized person and that timely, reliable access to data and information services is provided for authorized users.

Computer Network: Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Confidentiality: Protection of systems and data so that unauthorized parties cannot view the data, the property that sensitive information is not disclosed to unauthorized entities, and the assurance that information is not disclosed to unauthorized individuals or processes.

Controlled Unclassified Information (CUI): Information the Federal government owns or has created that needs to be safeguarded and disseminated using only controls consistent with Federal laws, regulations and policies.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An individual, who defines, manages, and controls the use of data and ensures compliance with the Information Security Standards with respect to the data.

Information Security: The policies, standards, guidelines, processes, activities, and actions taken to protect the confidentiality, integrity, and availability of information systems and the data they handle commensurate with sensitivity and risk.

Information Security Incident: means an adverse event or situation, whether intentional or accidental, that poses an enterprise impact or threat to the integrity, availability, or confidentiality of university data or systems or requires reporting based upon regulatory requirements.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control.

Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Intellectual Property: Please refer to the BOV POLICY # 35 (2019) INTELLECTUAL PROPERTY POLICY.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

Sensitive Information/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. Please refer to the 32-02 - Data Classification Policy

System Administrator: An individual or entity that implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An individual or entity responsible for the operation and maintenance of an IT system.

Technological Resources: 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.

Users: Faculty, staff and students as well as others who have been authorized to use Norfolk State University's technological resources, (e.g., contractors, interns, volunteers, etc.).

CONTACT(S)

The Office of Information Technology (OIT) officially interprets this standard. OIT is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Questions regarding this standard should be directed to OIT Security.

STAKEHOLDER(S)

University Faculty & Staff
Students
Others who have been authorized to use Norfolk State University's technological resources.

SYSTEM AND INFORMATION INTEGRITY (SI)

NSU-SI-1 FLAW REMEDIATION

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within 30 days of the release of the updates;
d. Incorporate flaw remediation into the organizational configuration management process;
e. Employ automated patch management tools to facilitate flaw remediation for system components and software;
f. Install security-relevant software and firmware updates automatically to system components where possible;
g. Remove previous versions of software and firmware components after updated versions have been installed; and
h. 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).

NSU-SI-2 MALICIOUS CODE PROTECTION

a. Implement signature or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available;
c. Configures malicious code protection mechanisms to:
    1. Perform periodic scans of the system on an organization-defined frequency and real-time scans of files from external sources at endpoint, network entry, and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and
    2. Block malicious code and send alert to administrator and Chief Information Security Officer in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

NSU-SI-3 SYSTEM MONITORING

a. Monitor the system to detect:
    1. Attacks and indicators of potential attacks; and
    2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system;
c. [Withdrawn: Not applicable to COV.];

d. Analyze detected events and anomalies;
e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
f. Obtain legal opinion regarding system monitoring activities;
g. Connect and configure individual intrusion detection tools into an information system-wide intrusion detection system; and
h. Employ automated tools and mechanisms to support near real-time analysis of events.

NSU-SI-4 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

a. Receive 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; and
c. Disseminate security alerts, advisories, and directives to personnel identified by name and/or by role.

NSU-SI-5 SPAM PROTECTION

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages;
b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures;
c. Automatically update spam protection mechanisms at least on a daily basis; and
d. Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

NSU-SI-6 INFORMATION INPUT VALIDATION

a. Check the validity of information inputs;
b. Review and resolve input validation errors within 30 days of discovery;
c. Verify that the system behaves in a predictable and documented manner when invalid inputs are received; and
d. Prevent untrusted data injections.

NSU-SI-7 ERROR HANDLING

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

NSU-SI-8 INFORMATION MANAGEMENT AND RETENTION

a. Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements;
b. Use the techniques to minimize the use of personally identifiable information for research, testing, or training; and

c. Use the following techniques to dispose of, destroy, or erase information following the retention period: in accordance with the Univerities Media Protection Policy.

NSU-SI-9 MEMORY PROTECTION

a. Implement malicious code protection controls to protect the system memory from unauthorized code execution.

NSU-SI-10 TAINTING

a. Embed data or capabilities in systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization.

EDUCATION AND COMPLIANCE

This standard shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

- Communicate the standard in writing, electronic or otherwise, to the University community within 30 days of approval;
- Post the standard on the appropriate website; and
- Educate and train all stakeholders and appropriate audiences on the standard's content, as necessary. Failure to meet the publication requirements does not invalidate this standard.

The Chief Information Security Officer (or designee) is responsible for official interpretation of this standard. Questions regarding the application of this standard should be directed to the Office of Information Technology. The Chief Information Security Officer reserves the right to revise or eliminate this standard.

Violations of this standard, including without limitation any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to comply with requirements of this standard may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may violate federal, state, or local laws.

EXCEPTIONS

Exceptions to this standard must be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Information Officer, and the Chief Information Security Officer.

REVIEW SCHEDULE

- Next Scheduled Review: 10/21/2026

- Approval by, date: OIT Standards Development Group, 10/21/2024

- Revision History: 10/21/2024,10/31/2025
- Supersedes: SEC530 Controls

RELATED DOCUMENTS

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx
32-02 - Data Classification Policy
https://www.nsu.edu/policy/admin-32-02.aspx
38-10 - Information Security Policy
https://www.nsu.edu/policy/bov-38-10.aspx