CONFIGURATION MANAGEMENT STANDARD (NSU-CM)

Standard Title:	**CONFIGURATION MANAGEMENT STANDARD (NSU-CM)**
Standard Number:	**38-10.#**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**CONFIGURATION MANAGEMENT (CM)**
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

STANDARD STATEMENT 1
DEFINITIONS 1
CONTACT(S) 3
STAKEHOLDER(S) 3
CONFIGURATION MANAGEMENT (CM) 4
EDUCATION AND COMPLIANCE 7
EXCEPTIONS 7
REVIEW SCHEDULE 7
RELATED DOCUMENTS 8

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.

CONFIGURATION MANAGEMENT (CM)

NSU-CM-1 BASELINE CONFIGURATION

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system:
    1. On an annual basis
    2. When required due to an environmental change; and
    3. When system components are installed and upgraded;
c. Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration; and
d. Monitors systems for security baselines and policy compliance.

NSU-CM-2 International Travel

a. All users traveling outside of the United States of America (including territories and military bases) with NSU property must notify the Office of Information Technology prior to leaving and have the property assessed for the compliance requirements listed in c;
b. All users traveling to federally embargoed and controlled countries must utilize a loaner device; and
c. The Chief Information Security Officer or designee will verify the loaner devices that will be used for international travel meet the following controls:
    1. All operating system security updates, web browser software, and any necessary application software have been installed;
    2. Infrared ports, Bluetooth ports, web cameras, and any hardware features, not needed for the trip, are disabled;
    3. If VPN is necessary, ensure it is installed and configured appropriately;
    4. All laptops and mobile telecommunications devices are encrypted, have sharing of all file and print services disabled, and have ad-hoc wireless connections disabled; and
    5. All required cables and power adapters are packed with the devices.

NSU-CM-3 CONFIGURATION CHANGE CONTROL

a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for a minimum of one year;

f. Monitor and review activities associated with configuration-controlled changes to the system;
g. Coordinate and provide oversight for configuration change control activities through Change Advisory Board that convenes on a regular basis to review significant changes prior to implementation;
h. Where possible, test, validate, and document changes to the system before finalizing the implementation of the changes; and
i. Require an information security representative to be a member of the Change Advisory Board.

NSU-CM-4 IMPACT ANALYSIS

a. Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice; and
b. After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

NSU-CM-5 ACCESS RESTRICTIONS FOR CHANGE

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

NSU-CM-6 CONFIGURATION SETTINGS

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization defined hardening standards;
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for system components based on operational requirements; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

NSU-CM-7 LEAST FUNCTIONALITY

a. Configure the system to provide only mission essential capabilities; and
b. Prohibit or restrict the use of functions, ports, protocols, software, and/or services that are not required for the business function of the system.

NSU-CM-8 SYSTEM COMPONENT INVENTORY

a. Develop and document an inventory of system components that:
    1. Accurately reflects the system;
    2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes organization-defined information deemed necessary to achieve effective system component accountability; and

b. Review and update the system component inventory on an annual basis and following an environmental change;
c. Update the inventory of system components as part of component installations, removals, and system updates;
d. Include in the system component inventory information, a means for identifying by name, position, and role, individuals responsible and accountable for administering those components; and
e. Provide a centralized repository for the inventory of system components.

NSU-CM-9 CONFIGURATION MANAGEMENT PLAN

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the system and places the configuration items under configuration management;
d. Is reviewed and approved by the Chief Information Security Officer or designee; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

NSU-CM-10 SOFTWARE USAGE RESTRICTIONS

a. Use software and associated documentation in accordance with contract agreements and copyright laws;
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work; and
d. Authorized open-source software must be actively maintained by the software community, cannot contain proprietary code, and must be distributed by a legitimate source.

NSU-CM-11 USER-INSTALLED SOFTWARE

a. The installation of software by users is prohibited;
b. Enforce software installation policies through organization-defined methods; and

c. Monitor policy compliance at least quarterly.

NSU-CM-12 SIGNED COMPONENTS

a. Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by 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: 10/21/2027
- Approval by, date: OIT Standards Development Group, 10/21/2024
- Revision History: 10/21/2024,10/23/2025,10/20/2026
- 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