PROGRAM MANAGEMENT STANDARD

Standard Title:	**PROGRAM MANAGEMENT STANDARD (NSU-PM)**
Standard Number:	**38-10.13**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**PROGRAM MANAGEMENT (PM)**
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
PROGRAM MANAGEMENT (PM) 4
EDUCATION AND COMPLIANCE 5
EXCEPTIONS 6
REVIEW SCHEDULE 6
RELATED DOCUMENTS 6

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.

PROGRAM MANAGEMENT STANDARD

PROGRAM MANAGEMENT (PM)

NSU-PM-1 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

a. Appoint a chief information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

NSU-PM-2 INFORMATION SECURITY AND PRIVACY RESOURCES

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;
b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and
c. Make available for expenditure, the planned information security and privacy resources.

NSU-PM-3 PLAN OF ACTION AND MILESTONES PROCESS

a. Implement a process to ensure that plans of action and milestones for the information security and privacy programs and associated organizational systems:
    1. Are developed and maintained;
    2. Document the remedial information security and privacy actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
    3. Are reported in accordance with established reporting requirements; and
b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

NSU-PM-4 SYSTEM INVENTORY

a. Develop and update at least on an annual basis an inventory of organizational systems, applications and projects.

NSU-PM-5 MEASURES OF PERFORMANCE

a. Develop, monitor, and report on the results of information security and privacy measures of performance.

NSU-PM-6 ENTERPRISE ARCHITECTURE

a. Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

NSU-PM-7 CRITICAL INFRASTRUCTURE PLAN

a. Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

NSU-PM-8 AUTHORIZATION PROCESS

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; and
b. Designate individuals to fulfill specific roles and responsibilities within the authorization processes.

NSU-PM-9 TESTING, TRAINING, AND MONITORING

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:
   1. Are developed and maintained; and
   2. Continue to be executed; and
b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

NSU-PM-10 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;
b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
d. Review and update policies and procedures at least on an annual basis.

NSU-PM-11 CONTINUOUS MONITORING STRATEGY

a. Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include establishing vulnerability and audit record coverage metrics to be monitored.

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: 10/21/2024,10/30/2025,10/21/2026
- 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