PLANNING STANDARD

Standard Title:	**PLANNING STANDARD (NSU-PL)**
Standard Number:	**38-10.12**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**PLANNING (PL)**
Approval Date:	**8/2/2024**
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.

PLANNING (PL)

NSU-PL-1 SYSTEM SECURITY AND PRIVACY PLANS

a. Develop security and privacy plans for the system that:
   1. Are consistent with the organization's enterprise architecture;
   2. Explicitly define the constituent system component;
   3. Describe the operational context of the system in terms of mission and business processes;
   4. Identify the individuals that fulfill system roles and responsibilities;
   5. Identify the information types processed, stored, and transmitted by the system;
   6. Provide the security categorization of the system, including supporting rationale;
   7. Describe any specific threats to the system that are of concern of the organization;
   8. Describe the operational environment for the system and any dependencies on or connections to other systems or system components, if applicable;
   9. Provide an overview of the security and privacy requirements for the system;
   10. Identify any relevant control baselines or overlays, if applicable;
   11. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for the tailoring decisions;
   12. Include risk determinations for security and privacy architecture and design decisions;
   13. Include security- and privacy-related activities affecting the system that require planning and coordination with organization-defined individuals or groups; and
   14. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Distribute copies of the plans and communicate subsequent changes to the plans to the System Owners and appropriate personnel;
c. Review the plans at least on an annual basis and following an environmental change;
d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
e. Protect the plans from unauthorized disclosure and modification.

NSU-PL-2 RULES OF BEHAVIOR

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
c. Review and update the rules of behavior at least on an annual basis and following an environmental change; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.
e. Include in the rules of behavior, restrictions on:
    1. Use of social media, social networking sites, and external sites/applications;
    2. Posting organizational information on public websites; and
    3. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

NSU-PL-3 SECURITY AND PRIVACY ARCHITECTURES

a. Design the security and privacy architectures for the system using a defense-in-depth approach.

NSU-PL-4 CENTRAL MANAGEMENT

a. Centrally manage defined controls and related processes.

NSU-PL-5 BASELINE SELECTION

a. Select a control baseline for the system.

NSU-PL-6 BASELINE TAILORING

a. Tailor the selected control baseline by applying specified tailoring actions.

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, 8/2/2024
- Revision History: 10/27/2025
- Supersedes: SEC530 PL 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