ASSESSMENT, AUTHORIZATION, MONITORING STANDARD (NSU-CA)

Standard Title:	**ASSESSMENT, AUTHORIZATION, MONITORING (NSU-CA)**
Standard Number:	**38-10.4**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**ASSESSMENT, AUTHORIZATION, AND MONITORING**
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
ASSESSMENT, AUTHORIZATION, AND MONITORING (CA) 4
EDUCATION AND COMPLIANCE 6
EXCEPTIONS 7
REVIEW SCHEDULE 7
RELATED DOCUMENTS 7

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.

ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

NSU-CA-1 CONTROL ASSESSMENTS

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
b. Develop a control assessment plan that describes the scope of the assessment including:
    1. Controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;
c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
d. Assess the controls in the system and its environment of operation at least on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
e. Produce a control assessment report that documents the results of the assessment; and
f. Provide the results of the control assessment to the Chief Information Security Officer and any other organization-defined individuals.

NSU-CA-2 INFORMATION EXCHANGE

a. Approve and manage the exchange of information between the system and other systems using Interconnection Security Agreements; Memoranda of Understanding or Agreement; or Nondisclosure Agreements;
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreement on an annual basis and following environmental changes.

NSU-CA-3 INTERCONNECTION WITH SENSITIVE SYSTEMS

For every sensitive agency IT system that shares data with non-Commonwealth entities, the agency shall require or shall specify that its service provider requires:

a. The System Owner, in consultation with the Data Owner, shall document IT systems with which data is shared. This documentation must include:
    1. The types of shared data;
    2. The direction(s) of data flow; and
    3. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Chief Information Security Officer (CISO), or equivalent, and the System Administrator;
b. The System Owners of interconnected systems must inform one another of connections with other systems;

c. The System Owners of interconnected systems must notify each other prior to establishing connections to other systems;
d. The written agreement shall specify if and how the shared data will be stored on each IT system;
e. The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data, including but not limited to, Data Breach requirements in this Standard;
f. The written agreement shall specify each Data Owner's authority to approve access to the shared data; and
g. The System Owners shall approve and enforce the agreement.

NSU-CA-4 PLAN OF ACTION AND MILESTONES

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
b. Update existing plan of action and milestones at least every 90 days based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

NSU-CA-5 AUTHORIZATION

a. Assign a senior official as the authorizing official for the system;
b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
c. Ensure that the authorizing official for the system before commencing operations:
    1. Accepts the use of common controls inherited by the system; and
    2. Authorizes the system to operate;
d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; and
e. Update the authorizations on an annual basis and following an environmental change.

NSU-CA-6 CONTINUOUS MONITORING

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organizational-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: organization-defined system-level metrics;
b. Establishing organization-defined frequencies for monitoring and organization-defined frequencies for assessment control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy. Metrics include monthly operating system scans, monthly database and web application scans, and independent assessor scans performed annually;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessments and monitoring information; and
g. Reporting the security and privacy status of the system to appropriate organizational officials at least every 120 days.

NSU-CA-7 PENETRATION TESTING

a. Conduct penetration testing on an annual basis and following an environmental change on any system housing University data.

NSU-CA-8 INTERNAL SYSTEM CONNECTIONS

a. Authorize internal connections of organization-defined system components or classes of components to the system;
b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
c. Terminate internal system connections after organization-defined conditions;
d. Review organization-defined frequency the continued need for each internal connection; and
e. Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

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