SYSTEM AND SERVICES ACQUISITION STANDARD

Standard Title:	**SYSTEM AND SERVICES ACQUISITION STANDARD (NSU-SA)**
Standard Number:	**38-10.16**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**SYSTEM AND SERVICES ACQUISITION (SA)**
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
SYSTEM AND SERVICES ACQUISITION (SA) 4
EDUCATION AND COMPLIANCE 4
EXCEPTIONS 9
REVIEW SCHEDULE 10
RELATED DOCUMENTS 10

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 SERVICES ACQUISITION STANDARD

SYSTEM AND SERVICES ACQUISITION (SA)

NSU-SA-1 ALLOCATION OF RESOURCES

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; and
b. Determine, document, and allocate the resources required to protect the system or system service as part of the organization capital planning and investment control process.

NSU-SA-2 SYSTEM DEVELOPMENT LIFE CYCLE

a. Acquire, develop, and manage the system using system development life cycle methodology that incorporates information security and privacy considerations;
b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
c. Identify individuals having information security and privacy roles and responsibilities;
d. Integrate the organizational information security and privacy risk management process into system development life cycle activities;
e. Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service;
f. Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service;
g. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments; and
h. Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

NSU-SA-3 NSU-SA-3

a. Project Definition:
    1. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.
    2. Incorporate IT security requirements in IT system design specifications.
    3. Verify that the IT system development process designs, develops, and implements IT security controls that meet information security requirements in the design specifications.
    4. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.
    5. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.
b. Implementation:

1. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.
2. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system if hosting or storing data classified as sensitive.
3. Require that the system comply with all relevant Risk Management requirements in this Standard.
4. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against information security risks and comply with the other requirements (see IT Systems Security Plans) of this document.

c. Disposition:
   1. Require retention of the data handled by an IT system in accordance with the agency's records retention policy prior to disposing of the IT system.
   2. Require that electronic media is sanitized prior to disposal, as documented (see Media Protection Standard), so that all data is removed from the IT system.
   3. Verify the disposal of hardware and software in accordance with the Media Protection Standard.

NSU-SA-4 NSU-SA-4

The Chief Information Security Officer is accountable for ensuring the following steps are documented and followed:

a. Application Planning:
   1. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.
   2. Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted.
   3. Security Requirements – Identify and document the security requirements of the application early in the development life cycle.
   4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:
      (a) Encrypted communication channels shall be established for the transmission of sensitive information;
      (b) Sensitive information shall not be transmitted in plain text between the client and the application; and
      (c) Sensitive information shall not be stored in hidden fields that are part of the application interface.

b. Application Development:

The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development:

1. Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.
2. Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.
3. University shall not use or store sensitive data in non-production environments (i.e., a development or test environment that does not have security controls equivalent to the production environment).
4. Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.
5. Default Deny – Application access control shall implement a default deny policy, with access explicitly granted
6. Principle of Least Privilege – All processing shall be performed with the least set of privileges required.
7. Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.
8. Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.

c. Production and Maintenance:

1. Production applications shall be hosted on servers compliant with the University's security requirements for IT system hardening.
2. Internet-facing applications classified as sensitive shall have periodic, not to exceed 90 days, vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

NSU-SA-5 ACQUISITION PROCESS

Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;
b. Strength of mechanism requirements;
c. Security and privacy assurance requirements;
d. Controls needed to satisfy the security and privacy requirements;

e. Security and privacy documentation requirements;
f. Requirements for protecting security and privacy documentation;
g. Description of the system development environment and environment in which the system is intended to operate;
h. Allocation of responsibilities or identification of parties responsible for information security, privacy, and supply chain risk management;
i. Acceptance criteria;
j. Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; and design and implementation information at the appropriate level of detail;
k. Require the developer of the system, system component, or system service to produce a plan for the continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization;
l. Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use;
m. Include organizational data ownership requirements in the acquisition contract; and
n. Require all data to be removed from the contractor's system and returned to the organization within a maximum of 30 days.

NSU-SA-6 SYSTEM DOCUMENTATION

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security and privacy functions and mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;
b. Obtain or develop user documentation for the system, system component, or system service that describes:
    1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
    3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;
c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent ; and
d. Distribute documentation to the appropriate organization-defined personnel.

NSU-SA-7 EXTERNAL SYSTEM SERVICES

a. Require that providers of external system services comply with organizational security and privacy requirements and employ correspondingcontrols;
b. Define and document organizational oversight and user roles and responsibilities with regard to external system services;
c. Employ processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis;
d. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services;
e. Verify that the acquisition or outsourcing of dedicated information security services is approved by the Chief Information Security Officer or designee;
f. Require providers of external system services to identify the functions, ports, protocols, and other services required for the use of such services;
g. Restrict the location of information processing; information or data; system services to locations within the Unites States of America based on the location of storing or processing of University data; and
h. Provide the capability to check the integrity of information while it resides in the external system.

NSU-SA-8 DEVELOPER CONFIGURATION MANAGEMENT

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service design, development, implementation, operation, and disposal;
b. Document, manage, and control the integrity of changes to the configuration items under configuration management;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes;
e. Track security flaws and flaw resolution within the system, component, or service and report findings to the Chief Information Security Officer;
f. Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components;
g. Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team;
h. Require the developer of the system, system component, or system service to enable integrity verification of hardware components;

i. Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions;
j. Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version;
k. Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies; and
l. Require the Chief Information Security Officer or designee to be included in the configuration change management and control process.

NSU-SA-9 UNSUPPORTED SYSTEM COMPONENTS

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

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, 10/31/2025,10/20/2026
- 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