SYSTEM COMMUNICATIONS PROTECTION STANDARD

Standard Title:	**SYSTEM COMMUNICATIONS PROTECTION (NSU-SC)**
Standard Number:	**38-10.17**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**SYSTEM AND COMMUNICATIONS PROTECTION (SC)**
Approval Date:	**7/3/2024**
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 COMMUNICATIONS PROTECTION (SC) 4
EDUCATION AND COMPLIANCE 7
EXCEPTIONS 8
REVIEW SCHEDULE 8
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.

NORFOLK STATE UNIVERSITY

SYSTEM COMMUNICATIONS PROTECTION STANDARD

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

NSU-SC-1 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

a. Separate user functionality, including user interface services, from system management functionality.
b. Store information from applications and software separately.

NSU-SC-2 SECURITY FUNCTION ISOLATION

a. Isolate security functions from non-security functions.

NSU-SC-3 INFORMATION IN SHARED SYSTEM RESOURCES

a. Prevent unauthorized and unintended information transfer via shared system resources.

NSU-SC-4 DENIAL-OF-SERVICE PROTECTION

a. Protect against or limit the effects of the following types of denial-of-service events: resource exhaustion, amplification attack, and types of denial-of-service events;
b. Employ the following controls to achieve the denial-of-service objective: application firewall and additional controls by type of denial-of-service events;
c. Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: all denial-of-service attacks except for system testing purposes;
d. Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks;
e. Employ monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: intrusion detection and application firewall; and
f. Monitor system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: system resources.

NSU-SC-5 RESOURCE AVAILABILITY

a. Protect the availability of resources by allocating resources by priority.

NSU-SC-6 BOUNDARY PROTECTION

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks;
c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture;
d. Limit the number of external network connections to the system;
e. Implement a managed interface for each external telecommunication service;
f. Establish a traffic flow policy for each managed interface;
g. Protect the confidentiality and integrity of the information being transmitted across each interface;

h. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

i. Review exceptions to the traffic flow policy at least on an annual basis and following an environmental change and remove exceptions that are no longer supported by an explicit mission or business need;

j. Prevent unauthorized exchange of control plane traffic with external networks;

k. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks;

l. Filter unauthorized control plane traffic from external networks;

m. Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces;
n. Prevent split tunneling for remote devices connecting to organizational systems;
o. Route internal communications traffic to external networks through authenticated proxy servers at managed interfaces;
p. Detect and deny outgoing communications traffic posing a threat to external systems;
q. Audit the identity of internal users associated with denied communications;
r. Only allows incoming communications from authorized sources to be routed to authorized destinations;
s. Implement host-based boundary protection mechanisms at the appropriate information system component layer;
t. Isolate information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system;
u. Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing;
v. Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device;
w. Prohibit the direct connection of system to a public network; and
x. Implement logically separate subnetworks to isolate critical system components and functions.

NSU-SC-7 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

a. Protect the confidentiality and integrity of transmitted information; and
b. Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

NSU-SC-8 NETWORK DISCONNECT

a. Terminate the network connection associated with a communications session at the end of the session or after 15 minutes of inactivity.

NSU-SC-9 **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**

a. Establish and manage cryptographic keys when cryptography is employed within the system in accordance with industry best practices for key management requirements;

b. Maintain availability of information in the event of the loss of cryptographic keys by users; and
c. Produce, control, and distribute asymmetric cryptographic keys using certificates issued in accordance with industry best practices.

NSU-SC-10 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: computer support that a user explicitly approves;
b. Provide an explicit indication of use to users physically present at the devices;
c. Provide physical or logical disconnect of collaborative computing devices in a manner that supports ease of use; and
d. Provide an explicit indication of current participants in all online meetings and teleconferences.

NSU-SC-11 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

a. Issue public key certificates under an approved certificate policy or obtain public key certificates from an approved service provider; and
b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

NSU-SC-12 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

NSU-SC-13 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER*)*

a. Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

NSU-SC-14 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

a. Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

NSU-SC-15 SESSION AUTHENTICITY

a. Protect the authenticity of communications sessions;
b. Generate a unique session identifier for each session with randomness and recognize only session identifiers that are system-generated; and
c. Only allow the use of approved certificate authorities for verification of the establishment of protected sessions.

NSU-SC-16 PROTECTION OF INFORMATION AT REST

a. Protect the confidentiality and integrity of the following information at rest: sensitive information; and

b. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on any system or system components: sensitive information based on confidentiality or integrity.

NSU-SC-17 PROCESS ISOLATION

a. Maintain a separate execution domain for each executing system process.

NSU-SC-18 DETONATION CHAMBERS

a. Employ a detonation chamber within systems supporting incident response activities.

NSU-SC-19 SYSTEM TIME SYNCHRONIZATION

a. Synchronize system clocks within and between systems and system components.

NSU-SC-20 CROSS DOMAIN POLICY ENFORCEMENT

a. Implement a policy enforcement mechanism logically between the physical and/or network interfaces for the connecting security domains.

NSU-SC-21 ALTERNATE COMMUNICATIONS PATHS

a. Establish alternate communications paths for system operations organizational command and control.

NSU-SC-22 SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

a. Implement software-enforced separation and policy enforcement mechanisms between security domains.

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: 7/3/2027
- Approval by, date: OIT Standards Development Group, 7/3/2024
- Revision History: 7/31/2025,7/31/2026
- Supersedes: SEC530 SC 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