# PHYSICAL ENVIRONMENTAL PROTECTION STANDARD

| | |
|---|---|
| **Standard Title:** | **PHYSICAL ENVIRONMENTAL PROTECTION (NSU-PE)** |
| **Standard Number:** | **38-10.11** |
| **Standard Reference:** | **COV SEC530 INFORMATION SECURITY STANDARD** |
| **Control Family:** | **PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)** |
| **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


STANDARD STATEMENT ..... 1
DEFINITIONS ..... 1
CONTACT(S) ..... 3
STAKEHOLDER(S) ..... 3
PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) ..... 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.

## PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)
## NSU-PE-1 PHYSICAL ACCESS AUTHORIZATIONS

Control:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals on an annual basis and following an environmental change;

d. Remove individuals from the facility access list when access is no longer required;

e. Authorize physical access to the facility where the system resides based on position or role;

f. Restrict unescorted access to the facility where the system resides to personnel with appropriate OIT clearances;

g. Temporarily disable physical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose; and

h. Disables physical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.

## NSU-PE-2 PHYSICAL ACCESS CONTROL

Control:

a. Enforce physical access authorizations at all physical access points including organization-defined entry/exit points to the facility where the system resides by;

   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress and egress to the facility using organization-defined physical access control systems or devices; guards;

b. Maintain physical access audit logs for all organization-defined entry or exit points;

c. Control access to areas within the facility designated as publicly accessible by implementing the organization-defined physical access controls;

d. Escort visitors and control visitor activity for organization-defined circumstances requiring visitor escorts and control of visitor activity;

e. Secure keys, combinations, and other physical access devices;

f. Inventory organization-defined physical access devices on an annual basis or more frequently if required and following an environmental change; and

g. Enforce physical access authorizations to the system in addition to the physical access controls for the facility at organization-defined physical spaces containing one or more components of the system.

**NSU-PE-3 ACCESS CONTROL FOR TRANSMISSION**

Control: Control physical access to cabling within organizational facilities using the appropriate organization-defined security controls.

**NSU-PE-4 ACCESS CONTROL FOR OUTPUT DEVICES**

Control: Control physical access to output from information system output devices to prevent unauthorized individuals from obtaining the output.

**NSU-PE-5 MONITORING PHYSICAL ACCESS**

Control:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs at least once every 90 days and upon occurrence of organization-defined events or potential indications of events;

c. Coordinate results of reviews and investigations with the organizational incident response capability; and

d. Monitor physical access to the facility and physical spaces containing one or more components of the systems using surveillance equipment at minimum.

**NSU-PE-6 VISITOR ACCESS RECORDS**

Control:

a. Maintain visitor access records to the primary and secondary data centers for a minimum period of one year;

b. Reviews visitor access records at least once every 90 days; and

c. Report anomalies in visitor access records to the Chief Information Security Officer and organization-defined personnel.

**NSU-PE-7 POWER EQUIPMENT AND CABLING**

Control: Protect power equipment and power cabling for the system from damage and destruction.

**NSU-PE-8 EMERGENCY SHUTOFF**

Control:

a. Provide the capability of shutting off power to the data center systems in emergency situations;

b. Place emergency shutoff switches or devices in organization-defined location by system or system component to facilitate access for personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

**NSU-PE-9 EMERGENCY POWER**

Control:

a. Provide an uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss; and

b. Provide an alternate power supply for the system that is activated manually and automatically and that is:

   1. Self-contained;

   2. Not reliant on external power generation; and

   3. Capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

**NSU-PE-10 FIRE PROTECTION**

Control:

a. Employ and maintain fire detection and suppression systems that are supported by an independent energy source;

b. Employ fire suppression systems that activate automatically and notify organization-defined personnel or roles and organization-defined emergency responders; and

c. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

**NSU-PE-11 ENVIRONMENTAL CONTROLS**

Control:

a. Maintain temperature and humidity levels within the data centers at organization-defined acceptable levels; and

b. Monitor environmental control levels on a daily basis

c. Employ organization-defined automatic environmental controls in the data centers to prevent fluctuations potentially harmful to the system; and

d. Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to organization-defined personnel or roles.

**NSU-PE-12 WATER DAMAGE PROTECTION**

Control: Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key

personnel.

**NSU-PE-13 DELIVERY AND REMOVAL**

Control:

a. Authorize and control system components entering and exiting the data centers; and
b. Maintain records of the system components.

**NSU-PE-14 ALTERNATE WORK SITE**

Control:

a. Determine and document the organization-defined alternate work sites allowed for use by employees;
b. Employ the following controls at alternate work sites: all equivalent controls of the primary site;
c. Assess the effectiveness of controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

**NSU-PE-15 LOCATION OF SYSTEM COMPONENTS**

Control:

a. Position system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access;
b. All information system components and services remain within the United States ;
c. All data and system information associated with the information system components and services remain within the Unites States;
d. All virtual components associated with an information system or service classified as sensitive with respect to confidentiality or integrity must reside in hypervisors that are hardened.

**NSU-PE-16 FACILITY LOCATION**

Control:

a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and
b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

**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: 8/2/2025
- Approval by, date: OIT Standards Development Group, 8/2/2024
- Revision History: N/A
- Supersedes: SEC530 PE 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