ELIZABETH CITY STATE UNIVERSITY
Physical and Environmental Security Policy

1. PURPOSE

The purpose of this policy is to define requirements for protecting Elizabeth City State University (ECSU) information resources from physical and environmental threat. This policy establishes minimum guidelines to protect the confidentiality, integrity, and availability of ECSU information resources accessed, managed, and/or controlled by ECSU.

2. SCOPE

This policy applies to all ECSU employees, whether full-time or part-time, paid or unpaid, temporary or permanent, volunteers, as well as to all other members of the ECSU community.

3. ACRONYMS / DEFINITIONS

Availability. The measures to which information and critical ECSU services are accessible for use when required.

Confidentiality. The measures to which confidential ECSU information is protected from unauthorized disclosure.

Information Resource. Data, information, and information systems used by ECSU to conduct ECSU operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

Information Security. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

Integrity. The measures to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of ECSU.

4. POLICY

A. PHYSICAL SECURITY THREATS

Employees and students that encounter a threat to their safety and well-being should immediately:

i. Move to a secure location.
ii. If on campus, report the issue to ECSU University Police.
iii. If off campus, report the issue to 911 emergency services.

B. SECURE AREAS

In addition to implementing technical controls to ensure the security and safety of ECSU information resources, controlling physical access to areas that house information resources are critical to ensuring those resources are properly secured. ECSU employees must protect physical areas under their control in a manner consistent with the sensitivity of the information resources located in that area. This policy applies to any information resource, regardless of the format (hard copy, electronic copy, laptop, server, network infrastructure, etc.).

It is the responsibility of all ECSU employees and students to take positive action to ensure physical security of ECSU facilities and locations. All visitors to restricted ECSU facilities must be authorized by the Chief Information Officer and/or Facilities Management and/or University Police while visiting a restricted location. Contact University Police for further assistance if you identify an unrecognized or unescorted person in a restricted location.

Physical access rights must be removed immediately for ECSU employees upon termination of their employment. These rights must also be modified accordingly when an employee change's role within ECSU. Temporary access may be granted to employees, contractors, or vendors when required for special circumstances. These temporary access rights must be properly revoked when the special circumstance has concluded.

All ECSU employees and students are responsible for understanding the appropriate access restrictions and guidelines for secure areas they access and are responsible for complying with these restrictions and guidelines to ensure these areas are appropriately secured.

C. EQUIPMENT SECURITY

ECSU will take reasonable action to protect ECSU equipment, including cabling, from physical and environmental threats, and unauthorized access. Equipment requiring special protection must be isolated or employ special physical protection according to need. Equipment must be reasonably and appropriately protected from power failures and surges as well as from heat, cold, and moisture.

When equipment has been damaged or has reached the end of its useful life, it must be disposed of securely, according to ECSU guidelines and procedures for asset disposal.

D. FACILITY PHYSICAL SECURITY

ECSU data centers, server rooms, and network routing facilities house servers and network equipment that process sensitive information and control access to the ECSU network. Physical access to these assets must be tightly controlled to protect them along with the information they house or process.

All ECSU data centers, server rooms, and network routing facilities must operate under a physical security monitoring program to protect the safety and security of the ECSU community and the information resources in these facilities. Precautions should be taken to ensure proper environmental alarms and backup systems are available to ensure critical components remain online.

5. PROCEDURES

ECSU shall develop, manage, and review operating procedures to create the proper security posture for protecting ECSU information resources. Such procedures shall be periodically reviewed as required.

6. COMPLIANCE / ENFORCEMENT / SANCTIONS

Any ECSU employee or student found to have violated this policy shall be subject to disciplinary action. Sanctions will be proportionate to the severity and/or frequency of offense and can include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

7. EXCLUSIONS / EXCEPTIONS

No approved exceptions exist at this time.