ELIZABETH CITY STATE UNIVERSITY
Network Management Security Policy

1. PURPOSE

The purpose of this policy is to ensure the correct and secure operations of ECSU (Elizabeth City State University) network information resources. This policy establishes minimum guidelines for ECSU Information Technology Services 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.

Principle of Least Privilege. This principle states a process will be granted only those privileges which are essential to perform its intended function.

4. POLICY

A. NETWORK MANAGEMENT

ECSU Local Area Networks (LAN) and Wide Area Networks (WAN) must be implemented, managed and supported by authorized Division of Information Technology (DIT) personnel. ECSU faculty, staff, and students are not permitted to connect any networking equipment (routers, switches, wireless routers, etc.) to ECSU networks without authorization from DIT personnel.

All networking equipment must be properly configured and maintained. All relevant security updates must be applied in a timely manner to ensure networking equipment is not vulnerable to exploit or compromise.

Physical access to network devices must be restricted to prevent unauthorized access. All physical locations housing network equipment must only be accessible to authorized personnel both during and after normal business hours.

Administrative access to network equipment must be carefully controlled and managed. All default user accounts and passwords on network equipment must be changed prior to implementation.

All network devices must have a hardened system configuration that includes disabling all unnecessary services. Access control lists or other access control / filtering technology should be implemented to limit network access to only the services that require it. Management interfaces must not be accessible directly from the Internet.

B. EXTERNAL CONNECTIVITY

External access to ECSU systems and services is provided for convenience and for effective and efficient service operation. In many cases, user-level access to services is facilitated directly via the Internet.

In general, remote access to ECSU internal networks is restricted to authorized ECSU staff and may only be facilitated via an approved VPN connection. Only approved devices are allowed to remotely connect to ECSU internal networks, and all VPN connections must be appropriately encrypted and require the use of an approved multi-factor authentication mechanism.

C. INTERNET ACCESS

Internet access is the backbone mechanism that allows ECSU to conduct its business and provide services to employees and students. As such, this access must be used appropriately as abuse causing disruption to Internet access can create serious service consequences for ECSU including, but not limited to its intranet resources. To ensure Internet access is available and properly utilized, DIT implements the following:

i. A firewall must be placed between internal ECSU networks and the Internet.

ii. Changes to policies defined on this firewall must be made in accordance with approved change management procedures. By default, all traffic through this firewall must be denied and policy changes will be made to allow specific traffic to pass through, in accordance with the Principle of Least Privilege. All policy changes to this firewall must be reviewed and approved by the Information Security Office/Officer (ISO) prior to implementation.

iii. Network connections will not be allowed to originate from the Internet and connect to systems on internal ECSU networks. These connections must terminate on a reverse-proxy (or similar system) configured for the purpose of providing this access, or the system must reside in a DMZ network that does not allow access to other internal systems. All connection architectures must be reviewed and approved by the ISO prior to implementation.

D. NETWORK SEGMENTATION

Network segmentation is an essential part of effectively managing risk in a networked environment. The following practices must be followed when segmenting networks:

i. Boundary protection mechanisms must not accept network traffic on “external” interfaces that appear to be coming from “internal” network addresses.
ii. Only proxies approved by IT Services management and the ISO will be installed on the boundary protection mechanisms.
iii. Configuration changes to boundary protection mechanisms must be reviewed and approved by the ISO prior to implementation.
iv. All configuration changes to boundary protection mechanisms must be performed in accordance with approved change control procedures.

E. NETWORK CONFIGURATION CONTROL

Changes to network topology or the configuration of any network device may only be performed by authorized DIT staff. All changes will be properly planned, approved, and implemented in accordance with approved change control procedures. Network devices must be properly maintained, updated, and secured by authorized DIT staff.

F. NETWORK ACCESS CONTROL

Access to ECSU’s production network and network infrastructure must be appropriately managed and controlled to ensure the network operates securely and efficiently. As such, the following requirements for accessing ECSU networks must be followed:

i. Access to ECSU networks must only be granted to authorized individuals using ECSU managed devices. Individuals are not permitted to connect personal or other non-ECSU-managed devices to internal ECSU networks.
ii. Vendors or other guests that require Internet access at ECSU facilities must utilize a separate network for the purpose of facilitating Internet access. This network must not have any connectivity to other internal ECSU networks.
iii. Administrative access to production network devices must only be granted to authorized ECSU staff members from DIT.

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.