FAYETTEVILLE STATE UNIVERSITY

NETWORK MANAGEMENT SECURITY

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	Information Technology
Applies to:	●Administrators ●Faculty ●Staff
History:	Issued – October 26, 2021
Related Policies/ Regulations/Statutes:	● *Physical and Environmental Security* ● *Information Systems Access Control*
Contact for Info:	Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this policy (Policy) is to ensure the correct and secure operations of Fayetteville State University (University) network information resources. This Policy establishes minimum guidelines for University Information Technology Services to protect the confidentiality, integrity, and availability of University information resources accessed, managed, and/or controlled by the University.

II. DEFINITIONS

The following definitions are used in this Policy:

- **Availability** shall mean degree to which information and critical College services are accessible for use when required.
- **Confidentiality** shall mean the degree to which confidential University information is protected from unauthorized disclosure.
- **Information Resource** shall mean data, information, and information systems used by the University to conduct University 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** shall mean 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** shall mean the degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the University.

- **Principle of Least Privilege** shall mean the principle that states a process will be granted only those privileges which are essential to perform its intended function.

III. NETWORK MANAGEMENT

The University's Local Area Networks (LAN) and Wide Area Networks (WAN) must be implemented, managed and supported by authorized University Information Technology Services (IT Services) staff. University employees and students are not permitted to connect any networking equipment (routers, switches, wireless routers, etc.) to University networks without authorization from IT Services staff.

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. See the University's *Physical and Environmental Security* policy for additional information.

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 account passwords must conform to the standards established in the University's *Information Systems Access Control* policy.

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.

IV. EXTERNAL CONNECTIVITY

External access to University 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 University internal networks is restricted to authorized University employees and may only be facilitated via an approved VPN connection. Only approved devices are allowed to remotely connect to FSU internal networks and all VPN connections must be appropriately encrypted and require the use of an approved multi-factor authentication mechanism.

V. INTERNET ACCESS

Internet access is the backbone mechanism that allows the University to conduct its business and provide service 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 the University. To ensure Internet access is available and properly utilized, IT Services implement the following:

- A firewall must be placed between internal University networks and the Internet.

- 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.

- Network connections will not be allowed to originate from the Internet and connect to systems on internal FSU 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.

VI. 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:

- Boundary protection mechanisms must not accept network traffic on "external" interfaces that appears to be coming from "internal" network addresses.

- Only proxies approved by IT Services management and the ISO will be installed on the boundary protection mechanisms.

- Configuration changes to boundary protection mechanisms must be reviewed and approved by the ISO prior to implementation.

- All configuration changes to boundary protection mechanisms must be performed in accordance with approved change control procedures.

VII. NETWORK CONFIGURATION CONTROL

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

VIII. NETWORK ACCESS CONTROL

Access to FSU's network and network infrastructure must be appropriately managed and controlled in order to ensure the network operates securely and efficiently. As such, the following requirements for accessing FSU networks must be followed:

- Access to FSU networks must only be granted to authorized individuals using FSU managed devices. Individuals are not permitted to connect personal or other non-FSU-managed devices to internal FSU networks.

- Vendors or other guests that require Internet access at FSU facilities must utilize a separate network for the purpose of facilitating Internet access. This network must not have any connectivity to other internal FSU networks.

- Administrative access to network devices must only be granted to authorized FSU staff members from IT Services.