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 ●Students
History:	Revised – February 4, 2025 Issued – October 26, 2021
Related Policies/ Regulations/Statutes:	● Physical and Environmental Security ● Information Systems Access Control
Contact for Info:	Vice Chancellor for Innovation, Technology Operations and Chief Information Officer | (910) 672-1200

I. PURPOSE

The purpose of this policy (Policy) is to ensure the protection and integrity of Fayetteville State University's (University) campus network, to mitigate the risks and losses associated with security threats to computing resources, and to ensure secure and reliable network access and performance for the University community. These actions are necessary so that the University can provide a reliable campus network to conduct the University's business and prevent unauthorized access to confidential and secure data. In addition, the University has a legal responsibility to ensure the security of its networks.

II. SCOPE

This Policy applies to all individuals who access the University's network computing resources through the following means. Devices include, but are not limited to workstations, laptops, tablets, smartphones, servers, consoles, controllers, and any other computing device capable of communicating on the University's network..

- devices which are used by individuals for network access, whether personally owned, University-issued or otherwise obtained,
- software connected to the University's network, whether installed on University devices or personally owned devices, and
- software used to store or process University data (whether it is connected or not connected to the University**'s** network).

III. NETWORK SECURITY

The University's networks must be implemented, managed and supported by authorized University Information Technology Services (ITS) staff. The following outlines the responsibilities of ITS related to network security.

A. Addressing and Domain Services

1. ITS is responsible for managing all Internet domain names related to the University (e.g., uncfsu.edu). Individuals, academic or administrative units may not create nor support additional Internet domain names without prior approval from ITS.

2. To ensure the stability of network communications, ITS shall be responsible for managing both the public and private IP address spaces in use by the University.

3. ITS may delegate administrative responsibilities to individuals for certain network ranges but retains the right of ownership for those networks.

B. Network Connections

The following are limitations on connecting to University networks.

1. Employees and students may not connect, nor contract with an outside vendor to connect, any device or system to the University's networks without the prior review and approval of ITS. University units desiring to provide Internet or other network access to individuals or networks not directly affiliated with the University must obtain prior approval from ITS.

2. To maintain reliable network connectivity, no University unit, regardless of the Unit's location, may deploy wireless routers, switches, bridges, and/or DHCP (Dynamic Host Configuration Protocol) services without prior review and approval of ITS.

3. Users are permitted to join the FSU secure network using ITS approved devices (e.g. laptops, desktops, tablets, etc.) only. All personal devices must use the FSU guest network and are permitted to connect those devices to the network under the following conditions:

    - the devices are used for University business.
    - the devices do not interfere with other devices on the network; or
    - the devices comply with all applicable University policies.

4. Unauthorized access to University networking equipment (firewalls, routers, switches, etc.) is prohibited. This includes port scanning or connection attempts using applications such as SSH/SNMP, or otherwise attempting to interact with university network equipment.

5. Unauthorized access to university equipment/cabling rooms is prohibited.

C. Wireless Network

The University will maintain a University-wide wireless network based only on IEEE 802.11 standards. The University-wide wireless network will be maintained a follows:

1. ITS shall be solely responsible for managing the unlicensed radio frequencies (wireless networking) on campus, which includes the 2.4 GHz and 5 GHz spectrum and may include future wireless spectrum standards, as defined by the IEEE, such as 60GHz.

2. ITS shall be responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on campus.

3. ITS shall collaborate with University units where devices used for specific educational and/or research applications may require specific support or solutions.

4. Due to interference in the operation of the University's wireless network, ITS shall prohibit unauthorized devices operating in the 2.4 GHz and 5 GHz spectrums. Such unauthorized devices shall include but not be limited to the following:

    - Wireless printers
    - MiFi devices or Wi-Fi hotspots
    - Wireless routers

D. External Traffic, Services, and Requests

The University's external Internet firewall default practice is to deny all external Internet traffic to the University's network unless explicitly permitted. To receive permission, University units must register systems, which require access from the Internet, with ITS. Users must request permission through a help desk ticket. Access and service restrictions may be enforced by device, IP address, port number, or application behavior.

ITS reserves the right to decrypt SSL traffic which transits the University network.

E. Security

1. The following measures have been implemented to ensure the security of the University's network:

    a. ITS may review any software which is written by University employees or students which is considered noncommercial or not generally accepted mainstream commercial if it is installed on University equipment or the network.

    b. If software does not have adequate security mechanisms, controls, and support, ITS reserves the right to prohibit the software or system from being connected to the University's network, installed on University computers, or used to store or process University data.

c. ITS may quarantine or disconnect any system or device from the University's network at any time that it is determined such is impacting regular network activity.

d. All devices connecting to the University's network must have adequate security installed in accordance with the University's published security policies.

e. Network appliances, virtual and physical, shall be monitored for updates and maintained in compliance with the ITS vulnerability management program.

2. Network usage judged inappropriate by the University is not permitted. Some activities deemed inappropriate include, but are not limited to the following:

a. Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCP or DNS servers; or a computer set up to act like such a device.
b. Engaging in network packet sniffing or snooping.
c. Setting up a system to appear like another authorized system on the network (trojan).

3. If a security issue is observed, it is the responsibility of University users to report the issue to their supervisor and ITS.

F. Access Control

Access to University resources requires a username and password. Passwords must be compliant with the University's Information Systems Access Control policy and other information security related policies. Individual user account passwords should not be shared with anyone.

To minimize the risk of compromised credentials, Multi-Factor Authentication (MFA) shall be required of Users who access the University's network resources. ITS recommends using "push notifications" by installing the MFA app on a smartphone. Faculty and Staff should promptly report to ITS the theft or loss of a device configured for MFA access to allow ITS to deactivate MFA for the device.

IV. MONITORING AND AUDITING

ITS reserves the right to monitor, access, retrieve, read, and/or disclose data communications when there is reasonable cause to suspect a University policy violation, criminal activity or upon a request from University management. Reasonable cause may be provided by the complaint of a policy violation or crime or as incidentally noticed while carrying out the normal duties of ITS staff.

ITS may perform assessments/audits of any University-owned devices or systems on its networks to determine the risks associated with protecting University assets. ITS may further perform non-intrusive security audits of any system or device connected to the University's networks to determine what risks the system may pose to overall information security. Additionally, ITS will maintain and monitor traffic logs for all network devices and systems for security auditing

purposes.

V. VIOLATIONS

The University reserves the right to test and monitor security, and to copy or examine files and information resident on University systems related to any alleged security incident or policy violation.

Attempting to circumvent security or administrative access controls shall be considered a violation of this Policy. Assisting others or requesting others to circumvent security or administrative access controls shall also be considered a violation of this Policy.

Any device found to violate this Policy or found to cause issues that may impair or disable the University's network or systems connected to it, may be immediately disconnected from the University's network. ITS may subsequently require specific security improvements, where potential security problems are identified, before the device may be reconnected.