Information Security Standard

Network Authentication and Authorization Standard

Initially Approved: September 9, 2021

Administering Office: Office of the CIO

I. Standard Statement

This standard operates under University Policy 117 Information Security. ISO 27002:2022 5.9 addresses the inventory and ownership of assets. This standard supports this control by requiring that all assets connected to the network authenticate in a way that identifies the asset owner or responsible party.

Additionally, ISO 27002:2022 8.20 requires that networks be managed and controlled to protect information in systems and applications. This control further suggests that network access should be authenticated and connection to the network be restricted. To comply with these requirements and to minimize the risk of unauthorized access to university data and systems all network access will be authenticated.

II. Scope and Application

This standard applies to all network connected devices except for wired ports in a residential setting and IT infrastructure including the data centers.

III. Definitions

802.1x - A network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network.
Network AAA System - Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, and auditing usage. In this context the network AAA system is the application that provides AAA services for the University's wired and WiFi networks.

IV. Network Authentication and Authorization Standard

a. Wireless network authentication will be enabled campus-wide
b. Wired network access will be enabled in all non-residential settings.
c. Authentication will be via the IEEE 802.1x standard

d. User-specific authentication is the desired control with device-specific (MAC) an acceptable alternative if technology compatibility issues, operational requirements (labs) or device limitations (IoT) preclude user-specific authentication.
e. Authorization to access certain network resources (controlled by placement into certain VLANs) will be based on policies configured and managed in the network AAA system.
f. After successful authentication the device will be placed in the appropriate VLAN based on the role configured in the network AAA system (e.g., faculty/staff, student, voice, building security, building control, etc.)
g. To allow for user's self-help and minimize disruptions to the campus operations in the event of a failed authentication or disruption of the network AAA system network access will result in a user or device being placed on the least privileged network available (Guest).

V. Responsibilities

It is the responsibility of all faculty, staff, and students to follow this information security standard. Failure to do so may result in the device being disabled on the network and possible disciplinary action.

It is the responsibility of the IT Division to enforce this standard.

VI. Exceptions

Exceptions to this standard for wired ports are allowed in limited IT work areas to enable imaging, troubleshooting, and other network activities not able to operate in an authenticated environment.

Further exceptions to this standard must be approved by the CIO or their designee and include compensating controls that reduce the risk of not following this standard.

VII. References

International Standards Organization (ISO/IEC 27002:2022, Clause 5 Organizational Controls)

International Standards Organization (ISO/IEC 27002:2022, Clause 8 Technological Controls)

University Policy 117 Information Security

University Policy 95 Data Network Security and Access Control