Auburn University at Montgomery
Policies and Procedures

Title: Wireless Network Policy

Responsible Office: Information Technology Services (ITS)

I. PURPOSE
The purpose of this policy is to outline procedures, processes and operational criteria to manage Auburn University at Montgomery's (AUM) wireless network and to ensure that these resources are used in a secure and efficient way.

II. POLICY
AUM has a commitment to provide wireless access to faculty, staff and students in a manner that maintains security at all levels. Wireless networks should not be considered as a replacement for a wired network but rather should be regarded as an extension to the existing wired network for general purpose access. ITS is charged with the responsibility for managing the network infrastructure of AUM including wireless networking.

III. EFFECTIVE DATE

July 1, 2007
Revised: February 6, 2008
Revised: May 1, 2023

IV. APPLICABILITY
This policy applies to all departments, faculty, staff, students and student workers, as well as contractors, vendors and visitors who access the AUM wireless network.

V. RESPONSIBILITY
ITS implements and administers the policy/procedure in detail.

Policy Responsible Office: Information Technology Services
Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS
N/A

VII. PROCEDURES

This section provides the general policy implementation guidelines:

- All wireless network devices and access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks.

- To ensure the integrity, reliability, and security of the AUM wireless network, ITS reserves the right to restrict access to services and resources that are

disruptive to the wireless network or pose a threat to the University's information security.

- Access to wireless network services will be restricted to AUM students, faculty, staff, and visitors that have been authorized for wireless service.
- ITS is the sole unit at AUM that can install or authorize install of wireless networking equipment for the AUM community. Wireless networking equipment not installed by ITS will be removed.
- ITS is responsible for establishing and maintaining standards for wireless access points.
- Wireless access points should not be used to access administrative application systems such as Student Banner that contain sensitive and confidential information.
- Faculty, staff or students who believe they have special wireless needs (e.g. research) must contact ITS before attempting to install any wireless device.
- Wireless networks will be secured by firewalls or segmented by access control policies that control the IP traffic on the network. The wireless network should be treated as a "foreign/untrusted network" from a security standpoint. Unauthorized traffic interception and/or bridging between the wired and wireless network is prohibited.
- Wireless users must abide by all applicable AUM IT Policies and procedures including the Information Technology Appropriate Use Policy.

VIII. SANCTIONS

AUM Wireless Network Access may be suspended if users violate this policy. Individuals who violate this policy may also be subject to further discipline in accordance with applicable conduct policies.

IX. EXCLUSIONS

NONE.

X. INTERPRETATION

The AUM Chancellor has the authority to interpret this policy.

APPROVAL TO PROCEED: _____ **DATE:** 4/18/23

APPENDICES

NONE