Auburn University at Montgomery
Policies and Procedures

Title: Wireless Network Policy

Responsible Offices: Information Technology Services

I. PURPOSE

This policy outlines procedures, processes and operational criteria to manage AUM's wireless network and to ensure that these resources are used in a secure and efficient way.

II. POLICY

Auburn University at Montgomery has a commitment to provide wireless access to AUM faculty, staff and students in a manner that maintains security at all levels. However, wireless networks should not be considered as a replacement for a wired network. It should be regarded as an extension to the existing wired network for general purpose access.

III. EFFECTIVE DATE

July 1, 2007

REVISED DATE

February 6, 2008

IV. APPLICABILITY

This policy applies to all AUM faculty, staff and students, who access the AUM wireless network.

V. RESPONSIBILITY

The CIO of Information Technology Services implements and administers the policy/procedures in detail.

VI. DEFINITIONS

802.11x: A family of specifications and standard for wireless networking.

Access point: The hub of a wireless network. Information to and from users of a wireless network go through access points.

Authentication: Process whereby AUM faculty, staff and students are verified to use the AUM wireless network.

*DHCP (*Dynamic Host Configuration Protocol): A protocol in which a server automatically assigns IP addresses so a user does not have to do this manually.

Hot Spot: A place where you can connect to a public wireless network.

*SSID (*Service Set Identifier) the network name that identifies a particular Wi-Fi access point.

*WLAN (W*ireless Local Area Network): The term often used for a wireless network within a limited area consisting of one or more wireless access points that provide network connectivity to computers equipped with wireless capability.

WPA (Wi-Fi protected access): An encryption system for preventing eavesdropping on wireless network traffic.

VII. PROCEDURES

A. All Wireless Network Devices and access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks.
B. To ensure the integrity, reliability, and security of the AUM wireless network, Information Technology Services 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.
C. Access to wireless network services will be restricted to AUM students, faculty, staff and visitors that have been authorized for wireless service. Wireless access points will only perform authentication for authorized users of the service.
D. Information Technology Services is the sole unit at AUM that can install wireless networking equipment for the AUM community. Wireless networking equipment not installed by ITS will be removed.
E. Students are explicitly not authorized nor permitted to install or operate WLAN access points in the residence halls.
F. Information Technology Services is responsible for establishing and maintaining standards for **802.11x** wireless access points (equipment and installation) for use at AUM.

G. Information Technology Services will maintain a database of access points, their locations, the frequencies in use, and the circuit numbers connecting the access points to the university's network.
H. Wireless networks are not appropriate for high bandwidth applications such as video streaming. It is most suited for applications such as email and web browsing.
I. Wireless devices must not be used to access administrative application systems such as Banner, Banner Finance and Banner HR that contain sensitive and confidential information.
J. All access point and wireless client adapters on the AUM WLAN will use an SSID maintained by ITS.
K. All users of the AUM WLAN will be required to use wireless clients that are compatible with the WLAN authentication protocol supported by ITS.

VIII. SANCTIONS

Any effort to circumvent the security systems designed to prevent unauthorized access to any AUM wireless network may result in suspension of all access to the wireless network. In addition, violations of this policy by AUM employees or students will be handled in accordance with the applicable faculty, staff and student policies.

IX. EXCLUSIONS

X. INTERPRETATION

The CIO of Information Technology Services will interpret this policy.

Approval to proceed: ________________________ Date: ______________