THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

WIRELESS NETWORKING AND GUEST ACCESS

Number 06.01.08

Division Administration – Office of Information Technology (OIT)

Date April 1, 2018; Reviewed/Revised April 28, 2025

Purpose The purpose of this policy is to establish the principles and security requirements to protect The University of Alabama in Huntsville's ("UAH" or "University") information technology (IT) resources from unauthorized access or inappropriate usage through the medium of wireless networking.

Policy Wireless networking offers increased convenience for mobile users. In order to ensure the security of university IT resources, wireless devices that use the campus wireless network must adhere to the same policies that govern all other IT resources. In addition, any wireless device on UAH's campus shall be configured as such to minimize wireless radio interference with UAH wireless network infrastructure, whether or not it is connected to the UAH wireless network.

Only wireless networking technologies installed by or under the auspices of the Office of Information Technology (OIT) are allowed to be connected to The University of Alabama in Huntsville (UAH) network. Installing network extension technologies such as wireless access points is prohibited without the express approval of OIT.

1.0 Extension of UAH Data Network

The UAH network shall not be extended by anyone other than OIT without written approval of the UAH Chief Information Officer (CIO) or their designee. This applies to both wired and wireless extensions of the UAH network.

2.0 Disruption of UAH Networks

Several categories of devices use radio frequencies in the same range as wireless networking technologies. Devices that use these frequencies could disrupt wireless network communications. Such devices include, but are not limited to media streamers, cordless phones, microwave ovens, and personal network devices. This interference can be intermittent and difficult to diagnose. OIT will work to resolve frequency conflicts, but cannot be responsible for resolving problems resulting from non-approved wireless devices. If a device installed on the university's campus by an individual or unit interferes with the wireless network maintained by OIT, the owner of the device must cooperate to resolve the conflict (regardless of whether the device is or is not connected to the university network). OIT may require relocation or removal of any disruptive Radio Frequency source or device.

Turning off or intentionally interfering with UAH wireless access is prohibited and considered a violation of the 06.01.03 Acceptable Use of IT Resources Policy.

3.0 UAH Wireless Network Names (SSIDs)

Only wireless access points that are approved by OIT are allowed to broadcast standard university SSIDs.

4.0 UAH Guest, Events and Conference Access

Accounts may be assigned to individuals not affiliated with UAH only in support of activities directly associated with UAH functions. A current full-time faculty or staff member must accept responsibility as the sponsor or contact related to the individual's activities while they are at the University. When requesting or renewing the account, this sponsor will provide information stating their relationship to the individual, outlining the individual's affiliation/benefit to UAH, and an indication that they understand their responsibilities related to the use of the individual account.

The UAH Help Desk will make the initial determination regarding eligibility of an individual to receive a UAH account. Cases where eligibility is unclear will be passed to the campus Chief Information Security Officer (CISO) for review and approval.

The UAH Help Desk will retain all documentation related to accounts while the account is active, and for one year following the point at which the individual is no longer associated with UAH, or from the point where the organization having a group account has been dissolved.

5.0 Exceptions

Requests for exceptions to this policy shall be submitted in writing to the OIT Help Desk. OIT will coordinate with the UAH Chief Information Officer (CIO) or their designee to review requests on a case-by-case basis as appropriate and will maintain a record of approved exceptions to this policy.

6.0 Compliance with Policy

OIT personnel may take immediate action to abate identified issues impacting network or system operations.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, the Staff Handbook, or university policy will be referred to appropriate university authorities.

Review The UAH CIO or their designee is responsible for the review of this policy every five (5) years (or whenever circumstances require).