THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

WIRELESS NETWORKING AND GUEST ACCESS

Number 06.01.08

Division Finance and Administration - Office of Information Technology (OIT)

Date April 2018

Purpose The purpose of this policy is to establish the principles and measures necessary to protect university IT resources from unauthorized access or inappropriate usage.

Policy This policy establishes the principles and measures to be taken to ensure that university IT resources are protected from unauthorized access or inappropriate usage through the medium of wireless networking.

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 information technology (IT) resources. In addition, any wireless device on UAH's campus shall be configured as such to reduce 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.

Procedure

1.0 Extension of UAH Data Network

As documented in the "Appropriate Use of IT Resources" policy, the UAH network shall not be extended by anyone other than OIT without written approval of the UAH Chief Information Security Officer (CISO) or one of his or her reports. This applies to both wired and wireless extensions of the UAH network.

2.0 Wireless Network Interference

Several categories of devices use radio frequencies in the same range as wireless Ethernet; therefore, other devices that use these frequencies may disrupt wireless network communications. Such devices include cordless phones, microwave ovens, and personal network devices using Bluetooth technology. 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-network 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).

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 identify himself or herself 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.

UAH Helpdesk 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 CISO for review and approval.

UAH Helpdesk 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.

Event or conference access to the UAH network shall be requested through the OIT Helpdesk at least 2 weeks in advance of event to allow for review of the request and if approved, time to configure needed access. Access shall be requested by a full-time employee of the university.

Network access charges may apply to conference or guest access.

5.0 Exceptions

Requests for exceptions to this policy shall be submitted in writing to the OIT Helpdesk. OIT will review requests on a case-by-case basis as appropriate and will maintain a record of approved exceptions to this policy.

6.0 Compliance of 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 IT Investment Advisory Council is responsible for the review of this policy every five years (or whenever circumstances require).