SOUTHERN
UNIVERSITY
WIRELESS NETWORK

Wireless Network

June, 2005 DoIT – POL – 002
Rev1: July 2018

July 12, 2018

The Division of Information Technology (DoIT) is responsible for the design, installation, and operation of the wireless network environment on the Southern University Baton Rouge Campus. This campus wide system will allow campus users to access campus information technology resources from mobile or portable computers.

In order to use the computer resources available at Southern University, students, faculty and staff must adhere to the policies and guidelines issued in the following document:

Policy of Information Technology Resources

Purpose

The purpose of this policy is to give an overview of the wireless campus requirements for Southern University and a brief introduction to the responsibilities of the university. It is to also define the policies and procedures for the use of the network services authorized by Technology and Network Services.

Scope

As authorized by Southern University Technology and Network Services policy, this document applies to all uses of Wireless Local Area Network (WLAN) technologies at all locations on the Southern University campus, both inside buildings and in outdoor areas, and to all devices connected to the Southern University network**.**

Policy and Procedures

1. Access to the wireless service will be restricted to current students, faculty, staff, and guests that have been authorized.

2. Students, faculty, and staff shall be authenticated with their Southern University Account (username and password). Guests will be provided a Guest login or limited access for authentication.

3. Users of the wireless service are responsible for obtaining a device that meets the current implementation requirements.

4. The Infrastructure and Network Operations (INO) is solely responsible for defining SSID's for the Southern University wireless network. Wireless equipment in University owned buildings or areas that are not part of the University wireless service shall not broadcast any text of their SSID associated with the University.

5. INO reserves the right to revoke wireless service authorization for any student, staff or faculty, guest, or for any device that is disrupting the operation of the wireless network. Violation of the Technology and Network Services policy or the Acceptable Use of Information Technology Resources policy will result in revocation of authorization to use the wireless network.

6. University faculty, staff, students and guests shall not install personal wireless networking equipment in University buildings or areas without written consent from INO. See items 3 and 4 in the implementation section for more information.

Implementation of the Policy

1. INO is responsible for configuring and managing the university's wired and wireless network as well as all connectivity to the network.

2. INO will be the sole provider of design, specification, installation, operation, maintenance, and management services for <u>all</u> wireless equipment.

3. Wireless devices/Access points are prohibited on the network without the permission of INO. Faculty, Staff and Students are explicitly not authorized or permitted to install or operate wireless access points, personal routers or hotspots in the office, classroom, common areas or residence halls.

4. Only wireless equipment installed and configured by INO personnel are permitted on the network.

5. A site survey by INO must be done prior to design and installation to ensure radio-frequency integrity, optimum location for coverage and to facilitate connection to power and the wired data network, and to identify possible interference problems.

6. All wireless communications on the University network and all authenticated access to the University network servers (e.g. mail, secure web, file transfers, etc.) must follow the Technology and Network Services standard encryption protocol.

7. DoIT continuously is upgrading and deploying wireless throughout the Southern University campus, however; if a department wishes to pay for wireless before implementation in their area, they must contact DoIT for installation and design support and be responsible for all costs (e.g., hardware and software, wired network connection, and power to the devices). Wireless equipment installed in this manner will be installed, operated and managed by INO.

8. The University reserves the right to disable and/or remove any wireless equipment not installed or configured by INO personnel.