WIRELESS LOCAL AREA NETWORK POLICY

June 2005 TNS –POL - 002

Created June 17, 2005

The Office of Technology and Network Services (TNS) 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

a. The Campus Network Management (CNM) unit is responsible for configuring and managing the university's wired and wireless network as well as all connectivity to the network.

b. CNM will be the sole provider of design, specification, installation, operation, maintenance, and management services for all wireless Access Points.

c. Access points are to not be installed on the network without the permission of Campus Network Management. Students are explicitly not authorized or permitted to install or operate WLAN Access Points in the residence halls.

d. Only access points installed and configured by CNM personnel are permitted on the network. All access points must comply with all security features of the wireless network.

e. TNS is currently in the process of deploying wireless hot spots throughout the Southern University campus, however; if a department wishes to pay for wireless before implementation in their area, they must contact TNS for installation and

design support and be responsible for all costs (e.g., hardware and software, wired network connection, and power to the Access Point). Wireless equipment installed in this manner will be installed, operated and managed by TNS.

f. All access to restricted systems require authentication (e.g., insertion of username and password).

g. All IP-capable devices installed on the University network will be assigned an IP address by a DHCP server or statically assigned and maintained by TNS.

h. Technology and Network Services may filter network traffic to exclude malicious traffic on both an incoming and an outgoing basis. Malicious traffic may include viruses and unsolicited commercial e-mail.

i. 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.

j. A site survey by CNM 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.

k. The University reserves the right to disable and/or remove any access point not installed or configured by CNM personnel.