Southern University Law Center
Policy #IT0007

Title: Wireless Access And Control Policy

Authority: Department Original Adoption: 7/20/2007
Effective Date: 7/20/2007
Last Revision: 9/17/2012

1.0 Purpose:

SULC's wireless network enables mobile computing and provides network services in situations where wiring is extremely difficult to install, such as historical buildings and large open areas.

The purpose of the wireless policy is two-fold:

to assure students, faculty, and staff access to a reliable, robust, and integrated wireless network and to increase security of the campus wireless network to the extent possible.

documents policies, standards, and guidelines for best practice as they relate to providing and using SULC's wireless network. Specifically, the policy identifies user and service provider responsibilities, lists the industry wireless standards supported on campus, addresses frequency issues, stresses the importance of security, and provides guidelines and best practices to improve security.

2.0 Scope:

This policy applies to all SULC users with SULC owned or personally-owned computers, workstations, or personal digital devices used to connect to the SULC network via wireless methods. This policy applies to wireless connections used to perform work on behalf of SULC, or in conjunction with appropriate activities associated with the role of the user accessing wireless network resources.

3.0 Definitions:

User – SULC employees and students, contractors, vendors, and agents working under the auspices of the Law Center.

4.0 Policy:

Standards: SULC has adopted the following approved IEEE (Institute of Electrical and Electronics Engineers, Inc.) standard protocols for wireless networking:

- **IEEE 802.11b** provides 11 Mbps of shared bandwidth per access point using the 2.4 GHz radio frequency. 802.11b is supported in all public spaces.
- **IEEE 802.11g** provides 54 Mbps of shared bandwidth per access point using the 2.4 GHz radio frequency. 802.11g is supported in many public spaces and is always compatible with 802.11b.
- **IEEE 802.11a** provides 54 Mbps of shared bandwidth per access point using the 5 GHz radio frequency. 802.11a is not compatible with 802.11b or 802.11g and is not recommended for public spaces where connection to the SULC network is desired. 802.11a may be an appropriate choice for certain private network applications.

Frequency Use: The 2.4 GHz radio frequency used by 802.11b and 802.11g is an unlicensed shared spectrum band. The 5 GHz radio frequency is another unlicensed shared spectrum which is used by 802.11a access points. In addition, there are only three non-overlapping channels within the 802.11b and 802.11g specifications. Consequently, access points can interfere with each other and other communications devices or appliances if not administered or deployed properly. Microwave ovens and cordless telephones are prominent examples. ITSS Networks and Communications will manage the shared use of unlicensed radio frequencies for the campus community and has campus authority to resolve interference issues.

User Provided Equipment: Users are responsible for purchasing wireless clients or wireless Ethernet cards for devices connected to the campus wireless network. Specifications for wireless Ethernet cards are included in the ITSS section of the SULC website and is the recommended resource for obtaining 802.11b, 802.11g, and 802.11a Ethernet cards.

Security: Wireless networks are not as secure as wired networks. Security for wireless networks is evolving. ITSS is responsible for establishing security policies for wireless communications based on current best practices. All wireless network installations must comply with established security policies including campus-wide IP (Internet Protocol) addressing and DHCP (Dynamic Host Configuration Protocol) services.

Experimentation: ITSS continually tests new and emerging wireless technologies. Departments may test new technologies, but may not implement technologies that compete or interfere with the campus wireless network. Departments must notify ITSS of any new technology trials.

Service Spaces

Public Spaces

ITSS Networks and Communications is responsible for providing and upgrading wireless service in public
spaces for a robust, seamless, and integrated wireless network.

- Public areas include but are not limited to areas such as atriums, general-purpose classrooms, and outdoor areas.
- Only 802.11b and 802.11g are supported in public spaces.
- ITSS maintains a list prioritizing public areas for central funding. Departments may request ITSS wireless services in public areas not yet covered by central funding. When additional funding becomes available to expand the public wireless network, priority will be given to departmentally funded ITSS access points.

Wireless Service Providers

- Access points installed in public spaces, classrooms, etc. should be securely mounted or in places not easily accessible by the public.
- Access points installed in private spaces should be secured like other computing equipment (e.g. computers). For example, lock doors when the space is not in use.
- Only connect access points to an Ethernet jack or Ethernet switch. Hubs should not be used in wireless networking.
- Use 100 Mbps Ethernet where available when connecting 802.11g and 802.11a access points to the campus network.

- When installing an access point, change the default password immediately and change every access point password at least annually.
- Use static IP addresses for access points. Disable any DHCP functions built into an access point.
- Configure access points in bridging mode to the wired network. NAT (Network Address Translation) is not allowed.
- Configure all public access point SSIDs as SULC or JAG. Private access points may be configured with different SSIDs.
- Outdoor access points must only be installed by ITSS.
- ITSS employs directional antennas and other methods to reduce propagation of radio waves outside the perimeter of the campus.
- The best practices for firewalls are the same regardless of whether they are connected with a wired or wireless connection.
- Mac address access lists can be used to control access through wireless access points. ITSS will set up security in private areas using appropriately configured ITSS access points.
- Access points used in public spaces must be WI-FI certified.

Wireless Network Users

- Wireless should only be used for mobile computing. Anytime wired access is available, it should be used for increased security and performance.
- All campus network users must register with ITSS to obtain an login credentials. The purpose of this is for authentication of users and tracking users and devices, not to limit access. Guests must be registered by an employee or department. Guest logins should be issued for a limited period of time.
- Wireless users on campus must use DHCP.
- Static IP addresses are not recommended for wireless clients.