Wireless Access And Control Policy
Policy Number 8-0007

Responsible Unit: Information Technology	Effective Date: 5/20/2007
Responsible Official: Associate Vice Chancellor, Information Technology	Last Reviewed Date: 7/15/2019
Policy Classification: Information Technology	Origination Date: 5/20/2007

1.0 Rationale:

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 Policy 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 Compliance:

Failure to with the policy will result in progressive disciplinary action up to and including termination.

5.0 Procedure:

User Provided Equipment: Users are responsible for purchasing wireless clients or wireless Ethernet cards for devices connected to the campus wireless network.

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.

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 static IP addresses for access points. Disable any DHCP functions built into an access point.
- 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

- External parties may use the GUEST wireless network for general internet access.
- Requests for additional access to other network services via wireless must be submitted and approved by ITSS.
- Wireless users on campus must use DHCP.
- Static IP addresses are not recommended for wireless clients.

APPROVED: Lata Johnson **DATE: 7/15/2019**