# Wireless Access And Control Policy
# Policy Number 8-0007

| | |
|---|---|
| **Responsible Unit:**<br>Information Technology<br><br>**Responsible Official**:<br>Director and Chief Information Officer, Information Technology<br><br>**Policy Classification**:<br>Information Technology | Effective Date:<br>5/20/2007<br><br>Last Reviewed Date:<br>5/5/2025<br><br>Last Revised Date:<br>5/5/2025<br><br>Origination Date:<br>5/20/2007 |

## 1.0 Rationale:

Southern University Law Center (SULC) provides a campus-wide wireless network to enable mobile access to academic and administrative resources. This policy establishes guidelines to ensure secure, reliable wireless connectivity that supports the instructional, research, and operational missions of the Law Center.

The wireless policy has two primary goals:

- To provide students, faculty, and staff with dependable and secure wireless access.
- To promote best practices and security standards for wireless infrastructure and user behavior.

## 2.0 Policy Scope:

This policy applies to all individuals accessing the SULC wireless network using SULC-owned or personally owned devices. This includes laptops, smartphones, tablets, and other wireless-enabled devices used on campus for educational, professional, or administrative purposes.

## 3.0 Definitions:

User: Any SULC student, faculty member, staff member, contractor, vendor, or guest accessing the wireless network.

ITSS: Information Technology and Security Services - responsible for oversight of wireless network security and performance.
SSID: Service Set Identifier - the name assigned to a wireless network. It functions as the network's public identifier, allowing users to distinguish one wireless network from another when scanning for available connections.

## 4.0 Policy Compliance:

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

## 5.0 Procedure:

**Wireless Network Use and Responsibilities**

1. **User Responsibilities**

- Users are responsible for equipping personal devices with compatible wireless capabilities (e.g., Wi-Fi cards or wireless adapters).
- All users must access the wireless network using SULC-approved configurations, including the use of DHCP (Dynamic Host Configuration Protocol). Static IPs for client devices are not supported.
- Requests for wireless network access beyond general Internet use must be formally submitted and approved by ITSS.
- External visitors may access general internet services via one of the provided GUEST wireless SSIDs. Requests for expanded access or additional SSIDs for events must be submitted to ITSS a minimum of 24 hours in advance for approval.

**2. Security Standards**

- Wireless communication is inherently less secure than wired communication. ITSS will maintain current security protocols aligned with industry best practices.
- Users must not interfere with or attempt to modify the configuration of SULC wireless access points.
- Users may not attempt to establish independent wireless networks (such as mobile hotspots, personal routers, or ad-hoc configurations) using SULC network resources.
- Users may not share access to SULC's wireless network through personal device settings such as Wi-Fi bridging, tethering, or any form of signal rebroadcasting.
- Users must not attempt to bypass network security measures, including firewalls and access controls.
- All wireless installations must adhere to SULC’s campus-wide IP addressing scheme and security configurations.
- The disclosure of passwords, unauthorized sharing of access credentials, or installation of rogue wireless devices is strictly prohibited.

## 3. Equipment and Access Points

- Only ITSS approved wireless access points may be installed or operated on campus.
- Access points:
  - Must be securely installed in both public and private areas.
  - Must be WI-FI certified and connected only to approved Ethernet jacks or switches. Connections through hubs are not permitted.
  - Must have reside on the VLAN established for Wireless Access Points.
- Departments may not install wireless devices that compete with or interfere with SULC’s central wireless network.
- Outdoor access points must be installed and maintained solely by ITSS.
- ITSS may use directional antennas and other techniques to limit signal propagation outside campus boundaries.

**4. Public and Private Service Areas**

- ITSS is responsible for providing wireless coverage in designated public and high-use areas including classrooms, atriums, libraries, and outdoor campus zones.

- ITSS is responsible for providing wireless coverage in private and departmental spaces including offices and departmental common areas.
- All access points will be treated as sensitive equipment and physically secured.

**5. Private or Departmental Spaces**

- Access points in private or restricted areas must be treated as sensitive equipment and physically secured.
- ITSS will support wireless access

**6. Consequences of Inappropriate Use**

Failure to comply with this policy may result in:

- Suspension or revocation of network privileges.
- Disciplinary action per institutional policies.
- Legal consequences for violations of law, including unauthorized network activity.

**6.0 Policy History and Review**

New Policy was created 5/20/2007. Revised 5/5/2025. The policy is subject to a five-year policy review cycle and shall be reviewed by the Director and Chief Information Officer for Information Technology and any changes will be submitted to the Chancellor for approval.

7. P**ublication of Policy**

This policy is published on the Southern University Law Center website at www.sulc.edu.

8. **Policy Approval**

This policy was approved by the Chancellor on 5/5/2025.

Alvin Washington
Chancellor, Southern University Law Center

5/6/2025
Date