

Wireless Networking

Original Implementation: February 3, 2005

Last Revision: July 28, 2015

Purpose

Stephen F. Austin State University's (SFA's) wireless local area network (LAN) enables wireless computing and provides reliable and secure network services in many locations on campus. It is a complementary system to the campus wired network.

Scope

This policy applies to all uses of wireless LAN technologies at all physical locations of SFA, both inside buildings and in outdoor areas. It does not apply to cellular wireless technology.

All SFA wireless LAN policies will comply with university, federal, state, and local laws and regulations.

Responsibilities

Information Technology Services is responsible for implementing wireless LAN technology in compliance with campus network standards and also for resolving frequency interference issues. These responsibilities include, but are not limited to:

- being the primary provider of design, specification, installation, operation, maintenance, and management services for all wireless access points;
- managing all SFA-owned wireless equipment;
- servicing wireless access points, i.e., the service demarcation points, and the wired network to which they are attached; and
- identifying and authenticating all users connecting to the wireless LAN.

Individuals may not install or operate wireless access points on university-owned property, including residence halls and apartments.

Access

All SFA faculty, staff, and students are required to have a valid user identification and password to use the wireless LAN. Any employee at the university can sponsor a guest on the wireless network using the self-service application provided by Information Technology Services.

Security

All wireless access points and wireless client adapters will use a Service Set Identification provided by Information Technology Services to access any wireless LAN provided by SFA. SFA will encrypt all data.

Sanctions for Policy Violations

Applicable university discipline and/or discharge policies will be followed in imposing sanctions related to a violation of this policy, including limiting a user's access. In the event of an imposed restriction or termination of access to some or all university computers and systems, a user enrolled in courses or involved in computer-related work activities may be required to use alternative facilities. If such facilities are unavailable, the user bears the responsibility for failure to complete requirements for course work and/or job responsibilities.

Cross Reference: Computer and Network Security (14.2); Use of Electronic Information Resources (16.32); Computing Software Copyright (9.1); Digital Millennium Copyright (9.3); Texas Information Resources Management Act, Tex. Gov't Code Ch. 2054; 1 Tex. Admin. Code §§ 202.70-.76; Tex. Penal Code Ch. 33.

Responsible for Implementation: Provost and Vice President for Academic Affairs

Contact for Revision: Chief Information Officer

Forms: None

Board Committee Assignment: Academic and Student Affairs