
Wireless Network Policy

0.0 CONTENTS

- 1.0 Purpose
- 2.0 Definitions
- 3.0 Background
- 4.0 Support of the Wireless Network
- 5.0 Client Support for the Wireless Network

1.0 PURPOSE

The purpose of this policy is to provide a highly reliable and reasonably performing wireless network service while ensuring network security and integrity and minimizing the interference between the campus wireless network and other wireless technologies deployed throughout the campus.

2.0 DEFINITIONS

Wireless Network – one in which a ~~mobile~~-user can connect to a local area network through a wireless (radio) connection.

IEEE – (Institute of Electrical and Electronics Engineers) fosters the development of standards that often become national and international standards. Self-described as “the world’s largest technical professional society – promoting the development and applications of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members.”

802.11 – family of specifications for wireless networks developed by the IEEE. There are currently four specifications in the family: 802.11, 802.11a, 802.11b and 802.11g

802.11a – wireless network specification that uses the FCC unlicensed 5GHz National Information Infrastructure (U-NII) band.

802.11b – wireless network specification that uses the FCC unlicensed 2.4GHz Industrial, Scientific, Medical (ISM) band. This specification operates at 11Mbps.

802.11g – proposed wireless network specification that uses the FCC unlicensed 2.4GHz Industrial, Scientific, Medical (ISM) band. This specification is expected to support rates at or above 20Mbps.

802.1X – standard designed to enhance the security of wireless networks that follow the IEEE 802.11 standard. It provides an authentication framework for wireless networks, allowing a user to be authenticated by a central authority.

3.0 BACKGROUND

With the ratification of the 802.11b standard for wireless networking in 1999 and the subsequent proliferation of interoperable, affordable products that support that standard, wireless network technology has established itself as an important complement to the traditional wired data networks.

Mobile access to information improves our ability to communicate. Faculty, staff and students will have the ability to check email or their schedules from most places around campus. Access to the Internet will no longer be tied to a computer in an office, lab or classroom. Wireless network technology is also beneficial for gaining network access in locations that are difficult, expensive, or inconvenient to wire. Examples include large lecture halls, outdoor areas, conference rooms, etc.

Wireless networks have their limitations. For example, they are slower than wired networks. Wireless networks are also inherently insecure. Tools are readily available to capture someone else's communications, including passwords and other sensitive data. Wireless network users must take extra precautions and adhere to standards to ensure secure communications over a wireless network.

While the standard does allow a wireless network card from one vendor to connect to an access point from another vendor, the devices must all be carefully configured for this support. Every product also has proprietary features that don't interoperate. This is especially true when it comes to security and management. Consequently, wireless network standards and central management of the campus "air space" are necessary to protect valuable information resources and to ensure the highest degree of interoperability as one moves from one location to another on campus with a mobile device.

4.0 SUPPORT OF THE WIRELESS NETWORK

4.1 Administrative Computing and Telecommunication Services (ACTS) will be responsible for the planning, design, operation, maintenance and management of the wireless network. No other wireless networks (other than RESNET) will be permitted to exist without prior approval from ACTS where the campus wireless network is available. This will ensure that clients have uniform connectivity throughout most places on campus.

4.2 ACTS will manage the radio frequency spectrums specified in the IEEE 802.11 standard. Other devices operating in same radio frequency spectrums can cause interference with the wireless network. These devices include, but are not limited to, other wireless networking devices, portable cordless (non-cell) telephones, cameras, keyboards, mice, audio speakers, ad-hoc (peer-to-peer) networks and computers or other devices equipped with a wireless network adapter and software to act as an access point. Where conflicts exist, ACTS will work with the campus community to determine whether the device may still be accommodated without causing interference with the wireless network.

4.3 ACTS is responsible for performing site surveys to determine access to the wireless network. The purpose of the site survey is to identify possible interference problems for a specific location. ACTS must consult with the department that utilizes the location prior to performing the site survey.

4.4 ACTS will provide reasonable physical security for all wireless network equipment.

5.0 CLIENT SUPPORT FOR THE WIRELESS NETWORK

- 5.1 Access to the wireless network will be done utilizing the 802.1X standard.
- 5.2 Departments and/or individuals are responsible for purchasing mobile devices and any devices/software required to connect to the wireless network.
- 5.3 Helpdesk will be responsible for assisting faculty and staff with troubleshooting their connection to the wireless network.
- 5.4 The Student Support Desk will be responsible for assisting students and faculty/staff with personally owned devices with troubleshooting their connection to the wireless network.
- 5.5 Helpdesk will be responsible for training the various support departments on campus. Training will include basic wireless technology, how it was implemented and how to connect to the wireless network.

6.0 PROHIBITED DEVICES

- 6.1 In order for the College to provide the students, faculty and staff with a quality wireless data network on campus, the Information Technology Steering Committee has approved a policy that bans the use of 2.4GHz and 5GHz portable telephones on campus. This is due to the interference caused by devices operating in the same wireless communications spectrum. Cell phones are not affected by this prohibition.

Sponsor:	C. Zeberlein	August 28, 2002
Recommended:	DACTS/DAC	August 2002
Reviewed:	ITSC	October 2002
Reviewed:	FETC	December 10, 2002
Recommended:	DAC/DACTS	January 7, 2003
Approved:	Provost/Senior Vice President	March 2003