



# Wireless Network Infrastructure Plan

Version 1.0  
April 27, 2007

## Table of Contents

Executive Summary .....	3
Infrastructure .....	4
Security .....	4
Reliability .....	5
Suitability .....	5
Responsibilities .....	6
Communications Services .....	6
Campus Units and Departments .....	6
Glossary .....	7

## Executive Summary

Information Resources (IRES) has delegated Communications Services to be responsible for providing a secure and reliable campus network to support the educational and service mission of the university. Under this broad responsibility, Communications Services must foster enterprise network standards to meet the networking requirements of all campus constituencies and to limit access to network connections which do not conform to standard network protocols and security measures. The campus airwaves are considered an enterprise-wide resource that must be centrally managed and maintained in the same manner as the wired campus network. Wireless networks are not a substitute for wired network connections. Wireless should be viewed as an augmentation to the wired network to extend the network for general access to common and transient areas. Initially, wireless infrastructure utilized 802.11b technology; in 2006 802.11g became the standard. As technology evolves, Communications Services will design the wireless system for compatibility with as broad a user base as possible without compromising the security or reliability of the entire network.

Maintaining security of the wireless system is crucial. Therefore, access to the wireless system will be limited to individuals authorized to use campus and Internet resources. Also, access to university systems containing confidential information from the wireless network will require Virtual Private network (VPN) software to authenticate users against the campus Wildcat directory and encrypt all traffic to and from the wireless access point. In addition, Communications Services will manage the physical security of wireless access points to protect them from theft or unauthorized access to the data port. In order for the wireless system to be secure it must be reliable.

The success of any wide deployment of a reliable wireless network requires that all equipment that operates in the frequency spectrum be carefully installed, configured and monitored to avoid interference between components of different network segments and other equipment. Other equipment that can cause interference includes, but is not limited to, unauthorized access points, microwaves, cell phones, radios, cordless telephones, copy machines, surveillance cameras and high voltage audio speakers. Where interference between the campus wireless network and other devices cannot be resolved, Communications Services reserves the right to restrict the use of all devices in university-owned buildings and all outdoor spaces. In addition to monitoring for other devices, Communications Services reserve the right to evaluate devices (laptops, PDAs, etc) as they are connected to the network to ensure they are updated with the latest patches against known software vulnerabilities and running current anti-virus software. These steps will help secure and sustain a reliable wireless network.

The wireless infrastructure will be deployed at California State University, Chico to support administrative and academic applications. A strategy for the deployment of these systems is essential to:

- Prevent interference.
- Ensure wireless availability.
- Safeguard security of campus network systems.
- Ensure that a baseline level of service quality is provided to a diverse user community.

This strategy describes how wireless technologies are to be deployed, administered and maintained at California State University, Chico and is supported by EM 97-18, the Policy on Use of Computing and Communications Technology. The strategy couples the desire for campus constituencies to deploy wireless technologies with a central administrative desire to assure that all constituents be assured of deploying such systems with an acceptable level of service quality and security.

## Infrastructure

Campus responsibility for electronic communication resources resides with the Vice Provost for Information Resources (IRES).

- Wireless equipment and users must follow general communications policies. Wireless services are subject to the same rules and policies that govern other electronic communications services at California State University, Chico.
- Deployment and management of wireless access points on campus and the extended campus network is the sole responsibility of Communications Services.
- Any wireless access point operated by an individual or department is subject to removal from the network.
- Only hardware and software that meets campus standards and is approved by Communications Services will be supported for wireless access.
- The initial rollout of wireless access points utilized the 802.11b standard. In 2006, 802.11g is the standard currently being used. Other standards will be supported in the future as they become widely available.
- Though Communications Services will seek to design these systems for compatibility with as broad a user base as possible, we can not ensure that the wireless network will work with all hardware, operating systems and applications.

## Security

Maintaining the security and integrity of the campus network requires adequate means of ensuring that only authorized users are able to access and use the network. Wireless devices utilizing the campus wired infrastructure must meet certain standards to ensure only authorized and authenticated users connect to the campus network and that institutional data used by campus users and systems is not exposed to unauthorized viewers.

- General access to the network infrastructure, including wireless infrastructure, will be limited to individuals authorized to use campus and Internet resources.
- Access to university systems containing confidential information from the wireless network will require Virtual Private Network (VPN) software to authenticate users against the campus Wildcat directory and encrypt all traffic to and from the wireless access point.
- Although Communications Services will provide a VPN option for wireless network privacy, ultimate password and data protection is the responsibility of the application and user. See the following website for more information:  
<http://www.csuchico.edu/inf/security/Security%20Brochurev7.pdf>
- Communications Services will manage the physical security of wireless access points to protect them from theft or unauthorized access to the data port.

- Communications Services reserve the right to evaluate devices (laptops, PDAs, etc) as they are connected to the network to ensure they are updated with the latest patches against known software vulnerabilities and running current anti-virus software.

## Reliability

In a wireless environment, network reliability is a function of both the level of user congestion (traffic loads) and service availability (interference and coverage). The campus approaches the shared use of the wireless network in the same way it manages the shared use of the wired network.

The success of any wide deployment of wireless networking requires all equipment that operates in the frequency spectrum be carefully installed, configured and monitored to avoid interference between components of different network segments and other equipment. Other equipment that can cause interference includes, but is not limited to, unauthorized access points, microwaves, cell phones, radios, cordless telephones, copy machines, surveillance cameras and high voltage audio speakers.

- To protect the integrity of the wireless network, periodic surveying of the airspace may be required to identify potential interfering devices. Communications Services will also respond to reports of specific devices that are suspected of causing interference and disrupting the campus network.
- Where interference between the campus wireless network and other devices cannot be resolved, Communications Services reserves the right to restrict the use of all devices in university-owned buildings and all outdoor spaces.
- The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list:
  - (1) Instruction
  - (2) Administration
  - (3) Public access
  - (4) Research
  - (5) Personal

## Suitability

Wireless networks are not a substitute for wired network connections. Wireless should be viewed as an augmentation to the wired network to extend the network for general access to common and transient areas.

- Wireless access points provide a shared bandwidth. As the number of users increase the available bandwidth per user diminishes. Users are responsible for using their fair share of the wireless bandwidth resources.
- To ensure reasonable and equitable access, Communications Services reserves the right to manage the shared bandwidth.
- New plans for buildings and gathering areas should consider the need for and use of wireless networking, similar to the planning done currently for wired networking.

## Responsibilities

### Communications Services

- Create, maintain, and update wireless communications strategy, procedures, and standards.
- Manage and deploy all wireless communications systems.
- Resolve wireless communication interference problems.
- Inform wireless users of security and privacy policies, procedures, and standards related to the use of wireless communications.
- Monitor performance and security of all wireless networks and maintain network statistics as required to prevent unauthorized access to the campus network.
- Monitor the development of wireless network technologies, evaluate wireless network technology enhancements and, as appropriate, incorporate new wireless network technologies into the California State University, Chico network infrastructure.

### Campus Units and Departments

- Work directly with Communications Services to deploy wireless access points.
- Assure proper network security is implemented in departmental spaces.
- Inform wireless users of security and privacy policies and procedures related to the use of wireless communications.
- Keep Communications Services apprised of new and changing wireless requirements

Questions regarding the Wireless Network Infrastructure Plan please contact Scott Claverie, Director of Communications Services at [sclaverie@csuchico.edu](mailto:sclaverie@csuchico.edu) or by calling the office of Communications Services at 898-4616.

## Glossary

**Access Point** – Any piece of equipment that allows wireless communications using transmitters and receivers to communicate. These devices act as hubs and allow communications to your campus network.

**Baseline Level of Connection Service Quality** – Determined by factors that affect radio transmissions; such as distance from the access point, number of users sharing the bandwidth, state of the environment from which the transmission is taking place, and the presence of other devices that can cause interference.

**Coverage** – The geographical area where a baseline level of wireless connection quality is attainable.

**Interference** – The degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless transmission or completely eliminate it depending on the strength of the signal. Interference is caused by:

- Unauthorized access points
- Microwaves
- Cell phones
- Radios
- Cordless telephones
- Surveillance cameras
- High voltage audio speakers

**Security** – As used in this policy, not only includes measures to protect electronic communication resources from unauthorized access, but also includes the preservation of wireless resource availability and integrity.

**Wireless Infrastructure** – Refers to wireless access points, antennas, cabling, power, and network hardware.