UC Santa Cruz Wireless Access Policy

VERSION: 1.4 STATUS: *DRAFT* DATE: 26 APRIL 2004

STEWARD: Director, Network & Telecommunications Services Tad Reynales

AUTHORITY: Vice-Provost, Information Technology Services Larry Merkley

TERM: 3 years from adoption.

REVIEW: Academic Senate, Subcommittee on Computing & Telecommunications
ITS Security Team
UCSC Information Technology Committee
ITC Network & Telecommunications Advisory Subcommittee

Contents

1. Purpose

This policy describes how wireless network communication technologies are to be deployed, administered, and supported at UC Santa Cruz. The purpose is to assure that all constituents of wireless networks receive an appropriate level of service quality in respect to reliability, integrity, availability, and security. This policy supplements University of California and UC Santa Cruz electronic communications policies. The Wireless Access Policy is subject to campus review and oversight as chartered by the Provost.

2. Overview

Wireless networking can offer great benefits to the UC Santa Cruz community in the pursuit of its primary missions of education, research and service. Wireless networking has been in existence for a few years, but is still a relatively new technology. The growing availability of relatively inexpensive, consumer-oriented wireless technology, and its apparent ease of installation, could lead to an unacceptable, uncoordinated and unplanned growth of wireless networking on the campus.

Since wireless uses the "public" radio spectrum, it can no longer be acceptable practice to be allowed to install or operate wireless devices on the campus network without a clear and agreed policy outlining the roles and responsibilities of all parties. These roles not only include the installation and setup of such network devices but also their ongoing use.

The design of wireless networks, specifically the placement of wireless access points to maximize coverage area and to minimize interference with other access points or devices, is something that has to be addressed and planned at a campus-wide level. This document aims to set out a framework and policy to deal with these wireless infrastructure issues.

Security of wireless networks is always a major concern and requires adherence to policy and full cooperation when wireless networking is incorporated into a campus network infrastructure. The broadcast nature of radio transmissions could lead to the inadvertent exposure of confidential information from computers or other wireless-connected devices. It is not acceptable to include University confidential data in unencrypted radio transmissions. University confidential data includes student records, faculty or staff personnel records and passwords that provide access to University-owned computers or services. Systems must be designed so that users can access confidential data securely.

3. Definitions: Wireless Network Technology.

- **Wireless Network/LAN:** a local area network technology that uses radio frequency spectrum to connect computing devices to a wired port on a network
- **Wireless Access Point (WAP)**: A network device that serves as a common connection point for devices in a wireless network. WAPs use radio antennas instead of wired ports for access by multiple users of the wireless network. WAPs are shared bandwidth devices and are usually connected to the wired network.
- **Wireless Infrastructure**: The WAPs, antennas, cabling, power, and network hardware associated with the deployment of a wireless network
- **Cell:** the three-dimensional volume receiving wireless signal from a given WAP
- **Coverage:** The physical area where a level of wireless connectivity is available.
- **Channel:** The chosen frequency slot for communication between the user's end point and a wireless access point.
- **Client hardware/software**: The equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device.
- **IEEE**: the Institute of Electrical and Electronics Engineers, wireless standards body
- **Radio Frequency (RF) Interference:** The degradation of a wireless communication signal caused by electromagnetic radiation from another source. RF interference can slow down or block a wireless transmission depending on the strength of the interfering signal. The IEEE specification for wireless Ethernet connectivity includes 802.11b, 802.11a and 802.11g access points and client devices, which operate in the 2.4 Ghz or 5.8 Ghz frequency ranges. These ranges are also used by devices such as cordless telephones, wireless keyboards and cord-free headsets; microwave ovens can also produce interference. Therefore, these devices can interfere with wireless LANs if they are operated in proximity to WAPs or to wireless clients.

Security: The condition that provides for the confidentiality of data transmitted over a wireless network. Password protection and encryption can be used to protect the data.

SSID: Service Set Identifier, essentially a name that identifies a wireless network. All devices on a specific wireless network must know the SSID of that network.

- **Public radio spectrum** --The Industrial, Scientific and Medical (ISM) radio bands were originally reserved internationally for non-commercial use of RF electromagnetic fields for industrial, scientific and medical purposes. ISM bands are the 902 Mhz, 2.4 Ghz and 5.8 Ghz area of the unlicensed or "public" radio spectrum

4. Rationale: Need for Policy

There would be three major areas of risk with an ongoing ad-hoc deployment of wireless networks in the University.

Security: By their very nature, wireless LANs are accessible to anyone within range of an access point. Physical boundaries are no longer relevant if radio signals can propagate through or around them. If a WAP is connected to the campus network without restrictions, anyone with the proper equipment will be able to access the network. Furthermore, anyone with the proper equipment can spy on traffic and, without security, can see users' passwords as well as other confidential data. Security of wireless network installations has to be rigorously managed, along with other electronic communications.

RF Interference: There are a limited number of channels available to use to optimize wireless service availability. If wireless LANs are installed without coordination with others in the area, interference is likely. This may result in significantly degraded network performance for everyone. The design practice for wireless LANs will locate WAPs to maximize coverage while keeping cells from interfering with each other.

Part of the ongoing service management and maintenance is the adjustment of radio transmitter power levels to shrink cell size as wireless usage grows and more WAPs are deployed. This allows numerous smaller cells to provide more uniform performance to end-users as well as an overall improved transmission rate. Planning for low-power, high-density operation requires coordinated central control.

Management: All standards-compliant wireless equipment from reputable manufacturers will generally coexist despite variations in implementation. However, for a campus-wide wireless LAN infrastructure to be properly planned, implemented and managed, appropriate hardware needs to be chosen for deployment. Low cost 'consumer-oriented' devices which do not provide security and management features required for enterprise networks will not meet the campus' service objectives.

5. Scope of Policy and Statement of Authority

Scope: This policy applies to all wireless network devices that connect to UCSC's wired network. This policy applies to the UC Santa Cruz main campus, including all academic, administrative and residential buildings and all outside locations, and applies to faculty, staff, students and visitors. Off-campus University-owned or leased locations connected to UCSC's network are included as well.

Authority: The Vice Provost--Information Technology Services (ITS) is responsible for providing a secure and reliable campus wireless network to support the mission of the University. The VP-ITS, in accord with applicable University of California policies and procedures, is charged with the development, review, coordination implementation, oversight, and administration of all policies, procedures, practices, and protocols that pertain to wireless communication, including but not limited to coverage and access, security and privacy, infrastructure development and deployment, standards, scope of service, acceptable hardware and software, appropriate use, and charges. The VP-ITS has authority and responsibility for all matters pertaining to wireless communication not described below or not expressly reserved. Under this broad responsibility, the following campus-wide wireless network policies are established:

6. The Policy

A. Wireless access points must abide by all federal regulations pertaining to wireless devices. Furthermore, WAPs shall conform to recommended minimum security and management specifications as defined by ITS and other interested parties.

B. No wireless access points are allowed to be connected to the campus network without prior registration with ITS. Unregistered or "rogue" WAPs will be subject to network blocking or physical removal from the network if necessary.

C. As part of the registration process, the locations of and an official point of contact for all wireless access points must be registered with ITS. In general, this point of contact will be the designated Security Contact for the department or unit.

D. Allocation of channels, SSID and encryption standards must be agreed upon and authorized before deployment. Official campus SSIDs (such as "cruznet") are reserved and may not be used without registration and authorization from ITS.

E. All wireless LAN communications shall be encrypted. Users connecting with a secure client device will have full access to the campus network. Users connecting without a secure client device will be limited to access using secure protocols.

F. All wireless communication shall require user authentication with a UCSC ID (username and password) before granting access to the campus network and beyond. *Exception*: guest users will be allowed web access only, with restricted bandwidth, restricted network access and limited connection time.

G. Wireless networks must be designed and deployed to avoid any interference between competing devices in the electro magnetic spectrum. Other devices may mean

neighboring WAPs or other components using the radio spectrum such as cordless telephones* or competing technologies. In the event that a wireless device interferes with other equipment the local department should be expected to resolve the situation. Disputes over channel allocation should be handled by the official point of contact for that wireless access point. Where multiple units or departments are involved, ITS will act as arbiter or coordinator. The order of priority for resolving unregulated radio frequency spectrum use conflicts shall be as follows:

1st Priority	--	Life and Safety
2nd Priority	--	Instruction and Research
3rd Priority	--	Administration
4th Priority	--	Public Access
5th Priority	--	Personal Use

Physical security should be considered the joint responsibility of all parties when planning the location of wireless access points and other wireless network components.
**ITS recommends 900 Mhz cordless phones for campus use, since 2.4 Ghz cordless phones interfere with devices using both 802.11 b and 802.11g wireless networks.*

7. Roles and Responsibilities

ITS is responsible for the operation and management of campus network infrastructure. A natural extension to the fixed network currently in existence is a wireless network. In order to ensure reliability, integrity and interoperability between the wired and wireless domains it is the responsibility of ITS to ensure the design, management and appropriate use of the campus wireless infrastructure is in accordance with best practice and existing policies.

ITS shall act as overall coordinators and controllers of the campus wireless network. Deployment and management of wireless access points in common areas of the campus is the responsibility of ITS. Given the properties of wireless networks, this is most of the campus. Campus-wide wireless needs take precedence over departmental needs, except in specific cases of wireless research or instruction, where ITS will design around the lab.

Individual departments and IT staff within those departments shall, where appropriate, be responsible for the localized management and implementation of wireless access points and infrastructure for instructional or research purposes in non-public areas. Departments must conform to the UCSC Wireless Access Policy. Non-conforming departmental wireless networks and "rogue" wireless access points will be subject to remediation or removal as recommended by the Director, Network & Telecommunications Services.
It is the responsibility of the department, center or unit staff to be knowledgeable regarding the provisions of all UCSC policies, and to coordinate with ITS on security and abuse issues. Individuals and departments are expected to purchase in line with University purchasing policy and by seeking guidance from ITS. To that end, ITS will regularly publish updates on security standards and hardware and software compatibility.

8. Conformance with Existing Policies

ITS is authorized to take whatever reasonable steps are necessary to ensure compliance with this and other network-related policies that are designed to protect the integrity and security of the campus network. Specific attention is drawn to the University of California Electronic Communication Policy, the UC Business & Finance Bulletin IS-3, Electronic Information Security, and the UC Santa Cruz Network Blocking policy. Under the latter, ITS is authorized to block or disconnect users or devices that are in violation of policy.

If a serious security breach or network abuse is in process, or if RF interference endangers life and safety, ITS may disconnect the LAN immediately. NTS or the Security Team will attempt to contact the registered Security Contact or other technical point of contact prior to blocking a wireless user or device. In cases where network blocking is not sufficient to resolve problems, a wireless access point may be physically disconnected or removed.

9. Resolution of Grievances and Disputes

Grievances with this policy, or conflicts or disputes between ITS and any department, center or unit should be presented to the Director, Network & Telecommunications Services for resolution. Should a satisfactory resolution not be achieved, appeals may be directed to the Vice-Provost, Information Technology Services.

10. References and Related Documentation

A. Office of the President: University of California Electronics Communication Policy (http://www.ucop.edu/ucophome/policies/ec/).

B. UC Business & Finance Bulletin IS-3, Electronic Information Security (http://www.ucop.edu/ucophome/policies/bfb/is3.pdf) and Implementing Guidelines (http://www.ucop.edu/ucophome/policies/bfb/is3guide.pdf).

C. UC Facilities Manual (http://www.ucop.edu/facil/fmc/facilman/), which includes facilities policies, procedures, and guidelines.

D. http://www2.ucsc.edu/cats/sc/help/policies/blockproc.shtml

E. UCSC Policy & Procedures Manual

F. Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.