



DISTRICT INFORMATION SYSTEMS

West Valley College
14000 Fruitvale Avenue
Saratoga, CA 95070
(408) 741-2087

Mission College
3000 Mission College Blvd.
Santa Clara, CA 95054
(408) 855-5415

WIRELESS ACCESS POLICY Fall, 2005

PURPOSE (WHY THIS DOCUMENT WAS CREATED)

Information Systems strives to provide reliable and secure network access at West Valley-Mission Community College District. This policy establishes acceptable practices for access to and use of wireless networks within the West Valley-Mission Community College District. The goal of this document is to provide clear understanding of proper procedures and responsibilities for wireless network use.

A wireless access policy is needed:

- To support the academic mission of the Institution
- To limit interference with the District network infrastructure
- To promote greater security in campus networking overall

Wireless networking uses the shared resource of the unlicensed radio frequencies on campus. Careful planning is required to support the implementation of wireless access across campus.

This document will be reviewed on a regular basis to ensure an accurate representation of the wireless environment is portrayed.

SCOPE (LOCATIONS INCLUDED IN THE WIRELESS NETWORK ROLL OUT PLANS)

Wireless Local Area Network (WLAN) using the 802.11 standard is a quickly evolving technology. This wireless technology is by nature easy to deploy but highly sensitive to overlapping frequencies. Because of these characteristics, all wireless use must be very carefully planned, deployed, and managed in a centralized fashion to ensure basic functionality, maximum bandwidth, and a secure network. **Wireless networking is available on our network to augment the wired network. It is not a replacement for wired network connections.**

Wireless Network Access is currently available in the following locations:

1. West Valley College Library
2. West Valley College Campus Center
3. Mission College Library

Expansion of the wireless network will be planned and implemented as funds allow.

GUIDELINES

West Valley-Mission Community College District provides wireless access to computing and information resources for students, faculty, and staff, within institutional priorities and financial capabilities. Wireless networks operate on a shared and finite airspace spectrum. Information Technologies will regulate this airspace to ensure its fair and efficient allocation and to prevent collision, interference, and failure.

In order to assure the highest level of service to the users of the wireless network without adversely affecting overall networking needs, help from all members of the campus communities is required to minimize the potential interference with those devices. Accidental or intentional disruption of a wireless network will deprive others of access to important District resources. Any person connecting a wireless device to the District network is responsible for the security of the computer device and for any intentional or unintentional activities from or to the network pathway that the device is using. Users and system administrators must all guard against abuses that disrupt or threaten the viability of all systems. Access to information resources without proper authorization from the data owner, unauthorized use of District computing facilities, and intentional corruption or misuse of information resources are direct violations of the District Acceptable Use of Computing and Network Resources policy. Persons using wireless devices to connect to the wireless network must comply with the equipment standards as outlined in the Standards section of this document and the District's Acceptable Use of Computing and Network Resources policy.

Information Systems manages the shared use of the wireless radio frequency in the same way that it manages the shared use of the wired network. Users may not use network services that will interfere with the District network. Information Systems reserves the right to restrict the use of wireless devices on campus. **No one may deploy wireless network access points or other wireless service on campus.** IS may monitor use of the airspace for potential interfering devices, and any user of a specific device found actually causing interference and disrupting the campus network will be notified; such unauthorized devices may be blocked from network access. Information Systems reserves the right to restrict the use of all 2.4GHz and 5 GHz radio devices in district-owned buildings.

SECURITY

The District does not currently require wireless communications to be encrypted; therefore, such, encryption at the application layer is very strongly encouraged. Use of un-secure communications applications such as telnet and ftp are discouraged. We

encourage the use of secure communications applications such as SSH, FTPS, and HTTPS for example, when such options are available.

Individuals aware of any breach of information or network security, or compromise of computer or network security safeguards, must report such situations to the appropriate system administrator and to Information Systems within 48 hours of discovery. WVMCCD Information Systems, in coordination with appropriate WVMCCD offices, will determine if financial loss has occurred and if control or procedures require modification. When warranted by such preliminary review, WVMCCD Police Services, internal Audit, and other WVMCCD departments or law enforcement authorities will be contacted as appropriate.

Violation of any provision of this policy may result in:

1. restriction or termination of a system user's access to WVMCCD Computer and Network Resources, including the summary suspension of such access, and/or rights pending further disciplinary and/or judicial action;
2. the initiation of legal action by WVMCCD and/or respective federal, state or local law enforcement officials, including but not limited to, criminal prosecution under appropriate federal, state or local laws;
3. the requirement of the violator to provide restitution for any improper use of service; and
4. disciplinary sanctions, which may include dismissal or expulsion.

STANDARDS (ACCESS POINTS, WIRELESS CARDS, ETC.)

Access Points –Access Points are running 802.11a, b, & g.

Wireless Network Cards – The following wireless cards have been tested for reliability on our wireless network:

- Apple Airport and Airport Extreme
- Cisco Aironet 350 PC Card
- Linksys Wireless-G Notebook Adapter #WPC54G v.2
- D-Link AirPlus XtremeG Wireless Cardbus Adapter #DWL-G650
- D-Link Wireless 108G USB Adapter #DWL-G132

Wireless access cards not on this list may work, but have not been tested for reliability and connectivity by Information Systems.

YOUR RESPONSIBILITIES IN USING WVMCCD's WIRELESS

Wireless networks are a shared resource: the more users connected to a wireless access point, the less bandwidth available to each of them. Please be considerate of fellow community members. Downloading large files (movie trailers, MP3s, etc), streaming audio & video, and using file sharing services are better done with your wired connection.

Any person connecting a wireless device to the wireless network is responsible for the security of the computing device. Current operating system patches, anti-virus protection, and spyware protection with current signatures are advisable.

Cordless telephones, BlueTooth devices, and microwave ovens are an example of some devices that are known to interfere with wireless networks. We ask that users refrain from using those devices in the areas where wireless access points are installed.

There is no encryption of communications on the wireless network. You are responsible for making sure any transactions you execute on the wireless network are done on secure sites or with secure methods. Please refer to the previous Security section of this document for more information and examples of secure protocols we recommend using.

DEFINITIONS

- **WVMCCD:** West Valley Mission Community College District
- **802.11a:** One of three wireless networking specifications under the Wi-Fi rubric. uses the 5 GHz band and runs at 54 Mbps.
- **802.11b:** The most common of the three wireless networking specifications included in the Wi-Fi certification mark. 802.11b uses the 2.4 GHz band and runs at 11 Mbps
- **802.11g:** The newest of the three Wi-Fi specifications. 802.11g is backward compatible with 802.11b, thanks in part to its use of the 2.4 GHz band, and it runs at the 54 Mbps speed of 802.11a. Most new equipment uses 802.11g.
- **Access Point (AP):** refers to a device that acts as a base station for a wireless network and covers a geographical area
- **Band:** Another term for spectrum used to indicate a particular set of frequencies. Wireless networking protocols work in either the 2.4 GHz or the 5 GHz bands.
- **Bandwidth (or throughput):** The amount of data that can be transmitted in a given amount of time. Throughput is commonly measured in bits per second. (Although throughput is not really a measurement of speed, most people, including us, use the word "speed" when talking about a high-throughput network.)
- **FTP:** A common way of transferring files on the Internet, though it's primarily used for uploading these days. FTP stands for File Transfer Protocol.
- **FTPS:** A secure version of the File Transfer Protocol.

- **HTTPS:** A secure network protocol used by the Web, although it's also now used for many other services. HTTPS stands for Secure Hypertext Transfer Protocol.
- **Interference:** refers to the degradation of wireless communication caused by electro-magnetic radiation from another source
- **SSH:** A security system that lets you create encrypted tunnels for any Internet protocol via port forwarding. SSH stands for Secure Shell.
- **Telnet:** An unsecure Internet communications protocol that enables a computer to function as a terminal working from a remote computer.
- **Wi-Fi:** A certification mark managed by a trade group called the Wi-Fi Alliance. Wi-Fi certification encompasses numerous different standards, including 802.11a, 802.11b, 802.11g, WPA, and more, and equipment must pass compatibility testing to receive the Wi-Fi mark.

HOW TO CONNECT TO THE WIRELESS NETWORK

1. In one of the areas listed earlier in this document turn on your computer.
2. Make sure your wireless network card is active
3. Your TCP/IP settings should be set for address resolution via DHCP.
4. Close your network settings.
5. Open your browser.
6. At the login page enter the following information (this is case sensitive):
 - Login = Guest
 - Password = wireless
 - Click OK.
7. You are now logged into the wireless network and can use the Internet.