Chapter 310, Communications and Technology
Section 17, Wireless Communications
Date: 10/2/02
Supersedes: New
Responsible Department: Information and Educational Technology
Source Document: University of California Electronic Communications Policy

---

Exhibit A, Wireless Security Standards

I. Purpose and Scope

This policy describes how wireless technologies are to be deployed, administered, and supported at UC Davis. The policy assures that all constituents using wireless communication networks receive an acceptable baseline level of service quality in respect to reliability, integrity, availability, and security. This policy supplements the UC and UCD electronic communications policies.

II. Definitions

A. Access point--connection points between segments of a local area network (LAN), using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Similar to standard wired "hubs," access points are shared bandwidth devices and can be connected to the wired network via a network access module (NAM), allowing wireless access to the campus network.

B. Authentication--the process of securing the identity of an individual, currently based on a user account name and password. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

C. Authorization--the process of assigning individuals the permission to read, write, or modify system objects or execute transactions based on their identity.

D. Baseline level of connection service quality--the level of connection service quality determined by factors that can 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. Acceptable throughput levels should be specified within service level agreements. Performance specifications defining baseline levels of wireless connection service are available at http://wireless.ucdavis.edu.

E. Common area--public access areas and general conference rooms, open seating areas where members of the community may sit and work, cafes, lounges, general lecture halls.

F. Coverage--the geographical area where a baseline level of wireless connection service quality is attainable.

G. 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.

H. Privacy--the condition that is achieved when successfully maintaining the confidentiality of personal, student, patient, and/or employee information transmitted over a wireless network. Privacy rights and limits are discussed further in Section 310-16.

I. Security--as used in this policy, measures to protect electronic communication resources from unauthorized access and to preserve resource availability and integrity. University policy regarding information systems security is defined in the UC Business & Finance Bulletin IS-3.

J. Wireless communications network--a network that uses wireless infrastructure to transmit and receive data over the air, minimizing the need for wired connections. A wireless communications network affords both data connectivity and user mobility.

K. Wireless infrastructure--wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

III. Policy

A. General

The Vice Provost--Information and Educational Technology (IET) is responsible for providing a secure and reliable campus network to support the mission of the University (refer to Section 310-16). Under this broad responsibility, the following campuswide wireless policies are established:

1. Only hardware and software consistent with wireless standards approved by the Vice Provost--IET or designee shall be used for wireless access points. Organizational units and personnel of campus departments shall also consult unit/departmental policies for additional guidance for the use of wireless hardware and software. Access to patient information by departments and personnel located at the UC Davis Medical Center using wireless technologies must be coordinated with UCDMC Information and Communication Services.

2. All wireless access points shall be registered with the Vice Provost--IET or designee. In the event that a wireless device interferes with other equipment, the Vice Provost or designee shall resolve the interference as determined by use priority.

3. Deployment and management of wireless access points in common areas of the campus is the responsibility of the Vice Provost or designee.

4. New plans for buildings and gathering areas shall consider the need for and use of wireless networking, similar to the planning done currently for wired networking.

B. Interference management

All equipment that operates intentionally or inadvertently in the wireless frequency spectrum will be carefully installed and configured to avoid interference between components of different network segments and other equipment. Consistent with ensuring the management of interference:

1. The installation, management, and use of all wireless communication networks shall be consistent with Federal and State laws and regulations and with UC and UCD policy.

2. The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list:

a. Life and safety

b. Research

c. Instruction

d. Administration

e. Public access

f. Personal

3. IET will respond to reports of suspected devices causing interference and disturbing the campus network. Where interference cannot be resolved, the use of wireless devices may be restricted by IET.

C. Security

General access to the network infrastructure, including wireless infrastructure, will be limited to individuals authorized to use UCD and Internet resources. Exhibit A contains further information on security architectures for wireless networks.

1. Wireless infrastructure components will be protected from theft or unauthorized access.

2. The wireless infrastructure does not provide user authentication services or ensure data privacy. Applications using the wireless infrastructure must require their own authentication, authorization, and encryption mechanisms to be used by wireless clients.

3. Wireless networks are not a substitute for wired network connections. Unless using encrypted protocols, wireless devices shall not be used for connecting to UCD business systems such as human resources, payroll, student information, financial information, or other systems that transmit sensitive or confidential information or are critical to the mission of the University.

IV. Procedures

The following procedures for deployment of wireless infrastructure are essential for the reliability, integrity, availability, and security of the campus wireless infrastructure.

A. Wireless standards

IET will publish wireless operational standards for use by campus departments at http://wireless.ucdavis.edu. The standards will be reviewed quarterly and updated as necessary.

B. Wireless infrastructure in common areas served by IET

Departments that wish to provide wireless connectivity within a common area of the campus must contact IET for review, coordination, analysis, and approval of such installations. Service information, use instructions, FAQs, network outage notices, and other information for common area wireless network locations will be published by IET at http://wireless.ucdavis.edu.

C. Registration procedures

1. All new installations of wireless networks and those in service prior to the adoption of this policy must register via the online forms published by IET at http://wireless.ucdavis.edu. Wireless network registration information includes, but is not limited to:

    a. Use/purpose

    b. Component list

    c. Access point locations

    d. Projected coverage map

    e. Virtual local area network (VLAN) assignments

    f. Network address modules (NAMs)

    g. Wiring plan

    h. Power plan

    i. Physical and logical security provisions

    j. Authentication

    k. Use of encrypted protocols above 40-bit encryption

    l. User security awareness

    m. Security monitoring

    n. Technical contact

2. Coverage areas of registered wireless networks will be published at http://wireless.ucdavis.edu. Access to this information via the web will be available to authorized users. Coverage area information will include information such as network administrator contact, signal range, VLAN, and registered access point location.

D. Performance monitoring

1. IET will manage the use of the common area wireless network and departmental wireless networks as it does the wired network. Trouble reports will be logged, reviewed, and a technician dispatched as required.

2. Departmental wireless networks in conflict with policies and procedures outlined within this document may incur a labor charge should a technician be dispatched to make corrections in local wireless network implementations. Early registration of a wireless network may prevent the unnecessary dispatch of a technician to resolve wireless network problems.

E. IET development and/or support of departmental wireless infrastructure

Departments may request assistance from IET in the design and installation of a wireless system within their department space. A form for this purpose is available via http://wireless.ucdavis.edu. Departments may also request assistance from IET for the management and/or support of their existing wireless network. This request can be made through a department head memorandum to the Vice Provost--IET.

V. Responsibilities

A. IET

1. Develop/maintain/update wireless communications policy and wireless security standards.

2. Maintain a registration of all wireless networks and access points on campus.

3. Resolve wireless communication interference problems.

4. Manage and deploy wireless communications systems in common areas of the campus.

5. Approve standards for wireless communication hardware and software used by campus departments.

6. Approve departmental installations of wireless communication systems/access points.

7. Develop/maintain/update wireless communication network security policies.

8. Inform wireless users of security and privacy policies and procedures related to the use of wireless communications in common areas.

9. Provide assistance to campus units for the development, management, and deployment of wireless communication networks.

10. Monitor performance and security of all wireless networks within common areas and maintain network statistics as required to prevent unauthorized access to the campus network.

11. Monitor the development of wireless network technology, evaluating wireless network technology enhancements and, as appropriate, incorporating new wireless network technology within the UCD network infrastructure.

B. Department heads

1. Adhere to all applicable Federal, State, and local regulations, and UC and UCD policy pertaining to the installation and use of wireless infrastructure.

2. Manage access points within departmental space and assure proper network security is implemented. Where two or more departments share a common building, the department heads may jointly share responsibility for wireless access points in that building or request the Vice Provost--IET or designee to take responsibility for the wireless access points in that building.

3. Register wireless access point hardware, software, and deployments with the Vice Provost--IET or designee.

4. Inform wireless users of security and privacy policies and procedures related to the use of wireless communications.

5. Monitor performance and security of all wireless networks within departmental control and maintaining network statistics as required to prevent unauthorized access to the campus network.

C. Users

1. Use critical and essential campus applications, such as DaFIS and Banner, only under encrypted protocols when using the applications over the wireless infrastructure.

2. Adhere to all applicable Federal, State and local regulations, and UC and UCD policy pertaining to the use of wireless infrastructure.

VI. References

See Section 310-16 for additional related references.

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. UCD Policy & Procedure Manual (http://manuals.ucdavis.edu/PPM/about.htm):

1. Section 310-10, Telecommunications Services.

2. Section 310-16, Electronic Communications Policy.

3. Section 320-15, Records Disposition and Retention.

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