

## Wireless Security Standards

### I. Introduction

The use of wireless network technology must not reduce the availability, integrity, and confidentiality of critical and essential applications and/or the UC Davis computing network. Accordingly, any implementation of wireless network systems at UCD must comply with the security standards described below for authentication, authorization, monitoring, reporting, and user awareness.

### II. Authentication

Access to wireless network connectivity is limited to authenticated users (users whose identity has been verified). Authentication is performed using an encrypted message format to ensure confidentiality of authenticating information. Wireless user accounts may not be shared.

### III. Authorization

Due to the lack of privacy of network communication over existing wireless network technology, all wireless traffic is presumed to be insecure and susceptible to unauthorized examination. System and/or application access authorization under wireless network technology is limited as follows:

- A. Users are prohibited from using wireless network technology to access critical and essential applications, such as DaFIS and Banner, unless the wireless network communication is performed using encrypted protocols.
- B. Due to the inherent security weakness and lack of scalability of Wired Equivalency Privacy (WEP) and Server Set Identification (SSID), static WEP keys and SSIDs will not be acceptable as security measures.
- C. Wireless network users will employ encrypted protocols for transmitting sensitive and/or confidential information over a wireless network connection. These encrypted protocols include, but are not limited to, Secure Sockets Layer (SSL) for web communication; Secure Shell, Version 2 (SSH); and IP security protocol (IPsec).

### IV. Security Awareness

All wireless network users will receive instructional material via a written or web publication upon registration for authentication. The instructional web material (refer to <http://wireless.ucdavis.edu>) will include but not be limited to the following topics:

- A. Authentication for wireless network access and protection of passwords.
- B. Authorization for use of wireless network technology.
- C. Wireless interference issues.
- D. Privacy limitations of wireless technology.
- E. Procedures for reporting wireless network service problems.

- F. Procedures for responding to a suspected privacy or security violation.
- G. Procedures for revoking dynamic host configuration protocol (DHCP) registration due to termination of an affiliation with UC Davis.

The instructional web material will be provided via the website, except for security awareness information that is unique to the UCD unit hosting the wireless service.

## **V. Monitoring and Reporting**

The use of wireless network technology will be monitored on a regular basis for security and performance (monitoring responsibilities are defined in paragraph V of the policy).

- A. Authentication, authorization, usage, and wireless network performance reports are to be published on a daily, weekly, and monthly basis. The reports will provide the following information, but not be limited to:
  - 1. Access point availability.
  - 2. Incoming and outgoing traffic speeds by access points.
  - 3. Radio link performance.
  - 4. Successful and failed authentication attempts.
- B. The reports will be maintained according to the UC records disposition schedules or not more than five years.
- C. Any unusual wireless network event that may reflect unauthorized use of wireless network services will be immediately reported by the wireless system administrator to the campus Incident Response Team for review and, if appropriate, investigation. Further information about the campus Incident Response Team is available at <http://security.ucdavis.edu>.