



## OIT 62.408: Wireless Security

**Responsible Executive:** Information Security Officer  
**Responsible Office:** Office of Information Technology  
**Related Policy:**  
**Approved-On Date:** 2/28/2011  
**Effective Date:** 7/1/2011  
**Revision Date:** 2/1/2011

### I. Policy Statement

The Wireless Security Policy defines the steps necessary to provide adequate and effective protection for University wireless systems.

### II. Purpose

The Wireless Security policy defines the high-level specifications for the secure deployment and use of wireless networking.

### III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

### IV. Requirements

The University ISO is accountable for ensuring the following steps are followed and documented:

#### Wireless LAN (WLAN) Connectivity on the University Network

1. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal University network.
  - a. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);
  - b. WLAN infrastructure must authenticate client devices prior to permitting access to the WLAN;
  - c. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;

- d. Only University owned or leased equipment shall be granted access to an internal WLAN;
- e. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols ( i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
- f. Physical or logical separation between WLAN and wired LAN segments must exist;
- g. All University WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;
- h. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and
- i. WLAN clients will only permit infrastructure mode communication.

#### WLAN Hotspot (Wireless Internet)

- 2. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:
  - a. WLAN Hotspots must have logical or physical separation from the University's LAN;
  - b. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;
  - c. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and
  - d. Where University clients are concerned, WLAN clients will only permit infrastructure mode communication.

#### Wireless Bridging

- 3. The following network configuration shall be used when bridging two wired LANs:
  - a. All wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption methods (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
  - b. Wireless bridging devices will not have a default gateway configured;
  - c. Wireless bridging devices must be physically or logically separated from other networks;

- d. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;
- e. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and
- f. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).

## **V. Violations**

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

## **VI. Interpretation**

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.