

## **DHHS POLICIES AND PROCEDURES**

---

<b>Section VIII:</b>	<b>Privacy and Security</b>
<b>Title:</b>	<b>Security Manual</b>
<b>Chapter:</b>	<b>Wireless Security Policy</b>
<b>Current Effective Date:</b>	<b>12/2/05</b>
<b>Revision History:</b>	
<b>Original Effective Date:</b>	

---

### **Purpose**

The purpose of the Department of Health and Human Services (DHHS) Wireless Security Policy is to define the security requirements necessary to ensure the confidentiality, integrity and availability of all wireless communications that are used to transmit sensitive information.

### **Policy**

DHHS divisions/offices shall ensure the security of wireless communications by implementing the controls described below, which must minimally meet the standards adopted by the Office of Information Technology Services (ITS).

### **Roles and Responsibilities**

The DHHS Privacy and Security Office (PSO) is responsible for developing and maintaining standards, providing implementation guidelines, and providing security training. The PSO is also responsible for monitoring network security and enforcing the implementation of DHHS security policies, standards, and enterprise-wide procedures.

DHHS divisions/offices shall be responsible for managing their data and network resources which might include wireless communication devices. In some situations, the DHHS division or office may contract the Division of Information Resources Management (DIRM) or an outsourced entity to handle this responsibility.

- If DIRM manages a DHHS Division/Office ITS environment or application, DIRM shall be responsible for implementing the wireless security controls.
- If an outsourced contractor manages a DHHS Division/ITS environment or application, the Division/Office must ensure that the contractor implements the wireless security controls.

The DHHS Division/Office Information Security Officials (ISO) shall serve as the security point of contact for the organization. The ISO is primarily responsible for providing security oversight and reporting security-related incidents to the PSO.

## Implementation

Wireless networks enable computers to be interconnected using standard network protocols such as IP. Wireless networking technology relies on radio frequencies and data transmission. The most widely used wireless standard is the Institute of Electrical and Electronic Engineers (IEEE) 802.11 which has been adopted by the Office of Information Technology Services (ITS) to serve as the state-wide standard.

### Modes of Operation

Two (2) types of wireless networks are possible, and they differ on how wireless devices communicate with each other. Wireless LANs (WLANs) operate in either the ad-hoc or the infrastructure mode.

- Ad-hoc networks have multiple wireless clients communicating with each other as wireless peers to share data among themselves without the aid of a wireless access point (AP). This mode is also known as independent basic service set (IBSS).
- An infrastructure WLAN consists of several clients communicating with an access point which is usually connected to a wired network like a LAN. Most WLANs operate in infrastructure mode because they require access to the wired LAN to use services such as printers and file servers. This mode is also known as the basic service set (BSS).

All DHHS divisions/offices shall implement the following requirements:

1. **Approved Technology** – All wireless LAN access must be approved by the DHHS PSO. All wireless access points and base stations connected to the DHHS network must be documented and subjected to periodic penetration tests and audits. All wireless devices and the network interface cards used in DHHS computers must have a registered owner and be listed in the asset inventory for each DHHS division or office. If personally owned devices are used, the division/office must maintain an inventory of the registered owner and use.
2. **Physical Access** – All wireless devices shall be protected against theft, unauthorized use, or damage. For additional information, refer to the DHHS Physical and Environmental Security Policy. The following physical access requirements are part of the DHHS *Wireless Security 802.11 Statewide Information Technology Policy*:
  - All network access points and related equipment such as base stations and cabling supporting wireless networks shall be secured with locking mechanisms or kept in an area where access is restricted to authorized personnel.
  - The reset function on access points shall be accessible only to authorized personnel.

3. Network Access – Network access to DHHS information resources should be restricted only to those authorized. For additional information, refer to the DHHS Network and Telecommunication Security Policy. The following network access requirements are part of the DHHS *Wireless Security 802.11 Statewide Information Technology Policy*:

- Access points shall be segmented from an internal, wired LAN using a gateway device.
- The service set identifier (SSID), administrator user ID, password and WEP key shall be changed from the default value. Also, the SSID shall be configured such that it does not contain any identifying information about the organization.
- The SSID shall not contain characters that indicate the location of the wireless LAN access point or any other identifying name.
- The SSID broadcast function shall be disabled, except where technology does not permit. In cases where the broadcast SSID function cannot be disabled, the network administrator shall notify the DHHS division/office information security official. Access point response to ESS (Extended Service Set) should be disabled.
- A device shall not be connected to a wireless network unless it can provide the valid SSID.
- Devices used to access the state’s network over an IEEE 802.11 wireless connection shall have anti-virus software. Devices incapable of running anti-virus or firewall software such as radio frequency identification (RFID) tags, voice telephony systems, or personal digital assistants are exempt from this requirement.

The ITS wireless security IEEE 802.11 allows an exemption of personal firewalls. However, DHHS policies permit the security official to authorize any use of personal equipment or state issued equipment that does not meet specifications. An authorized representative of each operating unit or organization shall determine the level of security safeguards required, considering the security classification of the data accessed. However, the PSO must be consulted and concur with the level of security safeguards required.

- All access points shall require a password to access the administrative features. This password shall be stored and transmitted in an encrypted format.
- The ad-hoc mode for 802.11 communications (referred to as peer-to-peer mode or Independent Basic Service Set) shall be disabled by the network administrator. The ad-hoc mode shall be allowed only when an emergency, temporary network is required.
- Every device used to access the state’s network over a 802.11 wireless connection shall, when not in use for short periods of time, be locked (via operating system safeguard features) and shall be turned off when not in use for an extended period of time unless the design of the device is to provide or

utilize continuous network connectivity. Such items might include wireless cameras, RFID tag readers and other portable wireless devices.

- If supported, auditing features on wireless devices shall be enabled and resulting logs shall be reviewed periodically by designated staff.

4. Authentication – All DHHS users shall comply with the DHHS Authorization, Identification and Authentication Policy. All implementations must support a hardware address that can be registered and tracked (i.e., a MAC address). Access point level protection using MAC address filters for wireless devices shall not be used as a single authentication measure. All implementations must support user authentication in accordance to established procedures and standards. The following user authentication requirements are part of the DHHS *Wireless Security 802.11 Statewide Information Technology Policy*:

- All wireless access to the state’s network via an 802.11 wireless network shall be authenticated using the authentication standards defined by the DHHS PSO. Additional authentication shall also be performed through such technologies as SSL, SSH or VPN when a LAN is extended or access via a third party network using 802.11 wireless technology.
- 802.1X credentials for individual users shall be deactivated in accordance with an agency user management policy or within 24 hours of notification of a status change (for example, employee termination or change in job function).
- WAN authentication shall be performed when point-to-point wireless access points are used between routers to replace traditional common carrier lines.

5. Encryption – All sensitive DHHS wireless communication shall be encrypted. The following encryption requirements are part of the DHHS *Wireless Security 802.11 Statewide Information Technology Policy*:

A. Remote access to a state-owned intranet from a non-state-owned wireless network is allowed only if:

1. All end-to-end communications within the state’s intranet is encrypted using a proven encryption protocol with a minimum of 128-bit encryption. The encryption can be acquired and/or layered in a multitude of manners such as listed below or subsequent releases that have the ability to provide the required level of encryption.
  - a. Secure Socket Layer (SSL) within an Internet browser, i.e.,
  - b. Microsoft Internet Explorer 5.0x and Netscape Navigator 4.0x.
  - c. Virtual Private Network (VPN) communications between two of more hosts using Internet Protocol Security (IPsec).
  - d. Wireless medium 128-bit encrypted communications between the client (PDA / tablet PC, etc.) device and the wireless.

- e. Access Point (AP) using Wi-Fi Protected Access (WPA or WPA2).

It is important to note that; in order to secure wireless communications between the client device and the network there isn't a single solution. Many security measures can be layered to ensure the integrity of the data. All access from a non-state-owned wireless network to a state-owned intranet must meet the above criteria or access is not allowed.

Consult with your division security official or the DHHS Security Officer if in doubt, or further clarification of policies and procedures are required.

- Depending on the type of information traversing the wireless LAN, encryption is required at varying levels as noted in the ITS Wireless LAN Defense in Depth Architecture. At a minimum, public information requires WPA encryption and sensitive information requires 802.11i (WPA2) compliant AES encryption or at a minimum of 128-bit encryption. End-to-end encryption is highly recommended for sensitive data.
- When using WPA2, AES encryption shall be enabled and shall be no less than 128-bits.
- When using WPA, the highest level of encryption supported on the device shall be enabled.
- WPA encryption must use the temporal key integrity protocol (TKIP) or other IEEE or NIST-approved key exchange mechanism.
- WPA2 (802.11i) encryption must use Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) or other IEEE or NIST-approved key exchange mechanism.
- WEP encryption shall not be relied upon for wireless security.
- When end-to-end encryption is required across both the 802.11 wireless and wired network, then in addition to WPA2 (802.11i) data transmitted between any wireless devices shall be encrypted using a proven encryption protocol that ensures confidentiality. Such protocols include SSL, SSH, IPSEC and VPN tunnels.

Pre-Shared Keys (PSK) is the use of secret passwords or encryption keys that are entered into both sides of the message exchange ahead of time. Pre-shared keys are typed into the clients and servers (authentication servers, access points, etc.) or entered via floppy, CD-ROM or smart card. Pre-shared keys shall be strong in nature, randomly-generated and redistributed to users at least quarterly to protect against unauthorized shared key distribution or other possible key exposure situations. Pre-shared keys sent by email shall be encrypted. Key Management is the responsibility of the division/office or as outlined in the roles and responsibility section of this policy.

6. Wireless System Management - The following wireless system management requirements are part of the DHHS *Wireless Security 802.11 Statewide Information Technology Policy*:

- SNMP shall be disabled if not required for network management purposes.
- If SNMP is required for network management purposes, SNMP will be read-only with appropriate access controls that prohibit wireless devices from requesting and retrieving information.
- If SNMP is required for dynamic reconfiguration of access points to address AP failures and rogue access points, the SNMP protocol used shall adhere to SNMP Version 3 standards and only take place on the wired side of the network.
- Pre-defined community strings such as “public” and “private” shall be removed.
- The latest version of the SNMP protocol supported by both device and management stations shall be implemented and support for earlier versions of SNMP disabled.
- IEEE 802.11 wireless devices shall not be used to manage other systems on the network except in temporary, ad-hoc emergency situations or by use of end-to-end encryption with authentication.

7. Information Assurance – DHHS divisions/offices shall periodically review their wireless systems/networks to ensure that controls have been implemented and are effective in the following areas: confidentiality, authentication, availability, integrity, and non-repudiation. The following audit requirements are part of the DHHS *Wireless Security 802.11 Statewide Information Technology Policy*:

- Agencies using 802.11 wireless LANs must enable rogue access point detection in the management software of the WLAN if available and search their sites using wireless sniffers at least monthly to ensure that only authorized wireless access points are in place. More frequent reviews may be warranted based upon a completed risk assessment. This type of audit is also recommended for sites not using wireless technologies to detect rogue access points and end-user installed free agent access points.
- The management system shall monitor the air space for unauthorized access points and ad-hoc networks. If unauthorized devices appear, the management system shall allow personnel to take appropriate steps toward containment.

8. Wireless LAN Defense-in-Depth Architecture - All 802.11 wireless LAN implementations shall follow the guidelines specified in the defense-in-depth architecture documented in the DHHS *Wireless Security 802.11 Statewide Information Technology Policy*. A security plan shall be developed for all 802.11 wireless implementations. This plan shall include the LAN architectures, network

diagram, and the security controls implemented.

In accordance the DHHS security policies, each division/office security official shall review and approve all requests for wireless communication. All approvals shall be forwarded to the DHHS PSO. The DHHS Security Officer shall report all 802.11 wireless LANs to the State Chief Information Officer (SCIO).

## **Enforcement**

For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS security officer ([DHHS.Security@ncmail.net](mailto:DHHS.Security@ncmail.net)).

## **Exceptions**

Any exceptions to this policy will require written authorization. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Director of the Division of Information Resource Management (DIRM). The waiver request will be processed in accordance with the DHHS [IT Waiver and Appeals Policy](#).

*For questions or clarification on any of the information contained in this policy, please contact the policy owner or designated contact point: [DHHS Security Officer](#). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordination](#).*