State of Iowa Enterprise Wireless LAN Standard

December 11, 2008

Purpose

This standard establishes the minimum requirements for installation and operation of Wireless Local Area Networks (WLANs) for State of Iowa Agencies.

Overview

Wireless technology allows for mobility of computer equipment and users. The benefits of wireless networking, however, come with potential risks. Improperly configured wireless networks may allow unauthorized users access to agency systems and information. Unauthorized users may consume network bandwidth, degrade network performance, or use agency resources to launch attacks on other networks.

Scope

This document presents the minimum standards which must be met by agencies using wireless local area network technologies.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise WLAN Standard are defined below:

- **Access Point (AP):** A network device that allows devices, such as laptops, to communicate wirelessly and to connect to another network, typically an organization's wired infrastructure, the ICN, or a commercial Internet Service Provider.
- **Public Wireless Network**: A wireless network set up by a state agency to provide free Internet access to guests or the public. Public wireless networks are isolated outside of the logical and physical boundary of the agency network.
- **Service Set Identifier (SSID):** A unique identifier which differentiates one WLAN from another. All access points and all devices attempting to connect to a specific WLAN must use the same SSID.
- **Basic Service Set Identifier (BSSID):** A unique identifier for each wireless device. The MAC address used by a wireless access point.

Updates

This document will be reviewed at least every two years and updated as needed.

Enterprise WLAN Standard

The following minimum standards must be met for all WLANs:

1. **Policy**. Agencies shall establish a WLAN security policy.

2. **Registration.** Agencies shall notify the DAS Chief Information Security Officer prior to implementation of a wireless access point. The notification must include the following for each access point:
    a. Brand,
    b. Model,
    c. SSID and BSSID, and
    d. Physical location.

    The notification must also include the agency name and contact. Non-registered access points are not permitted and shall be removed from service.

3. **Separation of Wireless and Wired Networks.** Wireless network zones must be separated from wired network zones by a firewall or other packet filtering device.

4. **Critical Devices.** Servers and related devices critical to the operation of the agency are not allowed to be hosted from wireless network zones.

5. **Physical Protection.** Wireless access points must be physically protected to limit risk of theft, damage, unauthorized access or configuration reset.

6. **Passwords.** Strong passwords (i.e., alphanumeric with a special characters) shall be used. Two-factor authentication should be considered in addition to strong passwords.
    a. Default administrative passwords used to manage the AP shall be changed.
    b. Administrative passwords shall be at least 15 characters in length.
    c. User passwords to access the wireless shall be at least 8 characters in length.

7. **Access Point Configuration.** Access points shall, at a minimum, meet the following requirements:

    • **Encryption.** Access points purchased after the effective date of this standard must use WPA2-Enterprise or higher encryption. Encryption settings shall be set for the strongest encryption available in the product. Wired Equivalent Privacy (WEP) shall NOT be used.

    • **Service Set Identifier.** The SSID shall be changed from the factory default setting

    • **Beacon Intervals.** Beacon frames shall be set to the maximum interval length.

    • **Cryptographic Keys.** Default cryptographic keys shall be changed before implementation.

    • **Address Filtering.** Media Access Control (MAC) address filtering shall be enabled whenever possible. Only connections from recognized MAC addresses should be accepted by the AP.

    • **Simple Network Management Protocol Version 3.** If SNMP is needed Version 3 or later shall be used. The default SNMP community string must be changed to a strong community string. Privileges should be set to “read only” if that is the only access required. Unneeded access ports and protocols should be disabled.

    • **Channels.** Channels should be set to minimize interference.

    • **Range**. The radio frequency power level should be reduced to the minimum level needed and directional antennas used, where practical, to limit the access point range.

8. **Operating Logs.** Wireless access points, where possible, must be set to log operating events including: login attempts (both successful and failed), errors, and reboots. The logs should be maintained on a separate file server. Logs must be reviewed on a regular basis.

9. **Infrastructure Configuration:** The wireless access point shall be configured for infrastructure mode. Ad-Hoc mode allowing peer-to-peer communications between devices is not allowed.

10. **Intrusion Detection.** An intrusion detection/prevention system shall be used to detect unauthorized access attempts or inappropriate use.

11. **Updates**. All components shall have the latest security patches, upgrades and firmware updates.

12. **Assessment.** The DAS Information Security Office may assess state facilities to determine if unauthorized or improperly configured wireless local area networks are present and provide access to agency systems or information. Unauthorized WLANs shall be removed by the agency.

13. **Equipment Disposal**. All sensitive data and configuration information must be removed from wireless components before disposal. For example devices could be reset to factory default settings.

14. **Client Security Maintained.** All computers connecting to the wireless network intended for use by agency personnel must have a properly-configured, host-based firewall, up-to-date antivirus software and be compliant with applicable enterprise and agency standards. Software patches must be applied per the agency's patching schedule.

15. **Awareness Training:** Wireless users shall be provided with wireless security awareness training, including but not limited to documentation describing wireless computing risks.

16. **Public Wireless Network**. Public wireless networks established by agencies shall:
    a. Be isolated outside the logical & physical boundary of the agency network. For example be a separate feed provided by the ICN or a commercial ISP.
    b. Agencies may choose to require a user ID and password for access,

    Items 6c, 7, 8, 10, 14, & 15 of this standard DO NOT apply to public wireless networks but following them, where feasible, is encouraged.

Effective Date This standard shall be effective February 1, 2009.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation.