State of Iowa Enterprise Wireless LAN Security Standard

May 9, 2016

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 local area networks (WLANs) 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 standard applies to all participating agencies as defined by Iowa Code Chapter 8B.1(7). Non-participating agencies are encouraged to follow this and other enterprise standards.

Definitions

Selected terms used in the Enterprise WLAN Security 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 Iowa Communication Network (ICN), or a commercial Internet Service Provider.
- **Basic Service Set Identifier (BSSID):** Access Point MAC address(es).
- **Guest Wireless Network**: A wireless local area network set up by a state agency to provide Internet access to authorized guests. Guest wireless networks are isolated outside of the logical and physical boundary of the agency network.
- **Public Wireless Network**: A wireless local area network set up by a state agency to provide free Internet access to 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.

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 OCIO 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 shall be physically protected to limit risk of theft, damage, unauthorized access or configuration reset.

6. **Passwords.** Passwords shall meet the requirements of the Enterprise Authentication Security Standard and meet the following:

   a. Default administrative passwords used to manage the AP shall be changed.
   b. Administrative passwords shall be at least 15 characters in length.

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

   • **Encryption.** Access points 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 and controllers, where possible, must be set to log operating events including: login attempts (both successful and failed), errors, and reboots. The logs should be sent to central logging 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.** A wireless 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 State of Iowa - Information Security Office shall assess state facilities on the Capitol complex at least quarterly 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 shall be removed from wireless components before disposal.

14. **Client Security Maintained.** All agency computers connecting to Wireless Local Area Networks (WLANs) 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 receive wireless security awareness training, including but not limited to documentation describing wireless computing risks.

16. **Public Wireless Network**. Agency public wireless local area networks (WLANs) 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. Items 7, 10, 15 and 19 of this standard DO NOT apply to public wireless networks.

17. **Dual Connections**: Agency computers shall not connect to the agency wired network and Wireless Local Area Network (WLAN) simultaneously.

18. **Guest Wireless Networks**: Guest wireless users shall not directly connect to internal agency resources.

19. **Vulnerability Scanning**: Wireless Local Area Networks (WLANs) shall receive vulnerability scans at least monthly.

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

Effective Date This standard shall be effective May 9, 2016.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A) and Iowa Code 8B.21(1)(f)(2).

Variance Iowa Administrative Code 11 - 25.11(2) and Iowa Code 8B.21(5) provide for variances\waivers from security standards. Requests for a variance\waiver from any of the requirements of this standard shall be submitted in writing to the Chief Information Security Officer.