

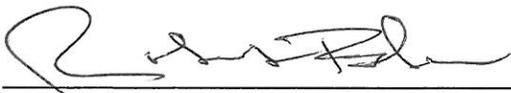


INFORMATION SECURITY AND PRIVACY POLICY

802.11 WIRELESS LOCAL AREA NETWORK

IT POLICY NUMBER: 2100-06

EFFECTIVE DATE: 12/05/2012

APPROVED BY: 
Robert Blair, Director
Department of Administrative Services

1.0 PURPOSE

This policy addresses the use, management, and control of 802.11 wireless local area network (LAN) technologies within the Department of Administrative Services (DAS). This policy addresses permitted and prohibited uses of 802.11 wireless local area network technologies within DAS facilities or for DAS business use.

2.0 SCOPE

This policy applies to all managers of DAS business units and IT systems that establish manage or use an 802.11 wireless local area network for the benefit of the Ohio Department of Administrative Services.

3.0 BACKGROUND

In Fiscal Year 2006, the Standards Subcommittee of the Multi-Agency CIO Advisory Council (MAC) established the Wireless Working Group (WWG) to research and recommend enterprise standards for wireless security that could help reduce potential vulnerabilities resulting from the availability of wireless technologies. Representatives from 17 state agencies and one state university joined to form the working group.

The WWG conducted comprehensive research and analysis focused on 802.11 technologies including surveys of agencies, state and professional organizations, discussions with industry analysts, manufacturers, and other states; and literature reviews of research publications, web sites, white papers and other published wireless security standards.

Research revealed that wireless local area networks based on 802.11 technologies can be a useful tool for enabling mobility across the enterprise; however, the security threats introduced into the enterprise by incorrectly designed or managed wireless networks can significantly outweigh the benefits.

Consequently, the main focus of the working group was identifying methods agencies should utilize to ensure reduced security risks to their wireless local area networks.

Research identified two design patterns—the *Hot Spot* and *Enterprise Mode* patterns—as models to explain the standards, guidelines and practices that must be put in place to ensure the safety and security of state assets when implementing an 802.11 wireless network. Each pattern, along with background information, guidelines and resource information, is provided in greater detail in *ITA-NET-01 802.11 Wireless Local Area Network Technical Architecture* available on the Internet: at www.ohio.gov/itp.

4.0 REFERENCES

- 4.1. **Ohio IT Standard; ITS-NET-01; 802.11 Wireless Local Area Network:** This state IT standard defines minimal requirements for the configuration and use of existing or newly implemented Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless local area networks within state government.
- 4.2. **Ohio IT Architecture; ITA-NET-01; Wireless Local Area Network Technical Architecture:** This document contains an introduction to wireless local area network security, wireless LAN security recommendations and guidelines for an 802.11 wireless LAN implementation.
- 4.3. **Ohio IT Standard; ITS-SEC-01; Data Encryption and Cryptography:** This state IT standard defines the minimum cryptographic algorithms that are cryptographically strong and are used in security services that protect at-risk or sensitive data.
- 4.4. **Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data:** This state IT bulletin provides guidance to agencies as they take steps to protect sensitive data and information.
- 4.5. **DAS Policy; 700-01; Information Technology Resource Usage:** This policy addresses permitted and prohibited use of IT resources in the DAS workplace and/or for DAS business.
- 4.6. A glossary of terms found in this policy is included in section **8.0 – Definitions**.

5.0 POLICY

DAS is issuing this policy to ensure compliance with related state policies and to protect DAS' IT resources. More detailed security standards and procedures supporting the implementation of this policy will be maintained separately.

All 802.11 wireless local area network technologies authorized to connect to the DAS network shall adhere to the following configuration, implementation and management requirements.

5.1 Network Configuration

- 5.1.1. 802.11 wireless networks shall be implemented in a secure manner consistent with Ohio IT Standard ITS-NET-01, "802.11 Wireless Local Area Network."
- 5.1.2. Access to state network assets from 802.11 wireless client devices shall be through wireless access points only (no peer-to-peer mode or ad-hoc connections are permitted except as may be indicated by DAS' disaster recovery and business continuity plans).
- 5.1.3. Hot Spot Mode installations using consumer grade wireless devices shall be physically separated from the rest of the state network using a firewall or like network appliance.
- 5.1.4. Enterprise Mode installations shall include logically separate wireless networks for guest and state user access each with a different and distinct broadcast identifier (Service Set Identification - SSID).
- 5.1.5. State sensitive network traffic shall be separated from unofficial visitor traffic using an encrypted connection over a virtual private network in accordance with Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data."

5.2 Wireless Access Point Devices

- 5.2.1. All wireless access point devices shall be owned by the state, no personally owned access point devices shall be connected to the network.
- 5.2.2. All wireless access point devices shall be industry certified by the Wi-Fi Alliance to guarantee interoperability and enterprise-level security capabilities.
- 5.2.3. The purchase and installation of all wireless access points shall be approved in advance by DAS/OIT/Infrastructure Services Division (ISD) Unified Network Services.
- 5.2.4. All access point devices shall be listed in a registry maintained by DAS/OIT/ISD Unified Network Services.
- 5.2.5. All default wireless access point names, usernames and administrator passwords shall be changed prior to installation. All wireless access points shall be named in a

manner consistent with the naming convention developed and managed by DAS/OIT/ISD Unified Network Services.

- 5.2.6. Access point devices shall include a broadcast identifier (SSID) in a format approved or assigned by DAS/OIT/ISD Unified Network Services.
- 5.2.7. All access points taken out of service shall be disposed of by DAS/OIT/ISD Unified Network Services who will ensure the removal of wireless access point configuration information – passwords, keys, names, network addresses and other pertinent information prior to disposal.
- 5.2.8. Upon the theft or loss of a DAS wireless access point, the access point configuration information in the remaining DAS wireless access points shall be changed by DAS/OIT/ISD Unified Network Services within 48 hours.

5.3 Client Devices

- 5.3.1. All state-owned client devices shall be Wi-Fi Alliance certified to guarantee interoperability and enterprise-level security capabilities.
- 5.3.2. DAS shall implement controls to ensure that wireless client devices authorized to connect to DAS networks, whether those networks are wireless or wired, are configured such that they may not connect to, or accept connection from, other wireless client devices in ad-hoc or peer-to-peer mode.
- 5.3.3. DAS shall implement controls to ensure that portable computing devices authorized to connect to DAS 802.11 wireless networks have personal firewalls and up-to-date anti-virus definitions and security patches.

5.4 Network Operations

- 5.4.1. The 802.11 access method or protocol for communication shall be an accepted and approved industry standard mechanism as defined by IEEE.
- 5.4.2. All data in transit on the wireless local area network, that is considered official or sensitive state information, shall be encrypted in a manner consistent with Ohio IT Standard ITS-NET-01, "802.11 Wireless Local Area Network."
- 5.4.3. When possible, access to the wireless local area network for official state business or access to sensitive information shall include client device and end-user authentication.
- 5.4.4. Authentication mechanisms or protocols selected are to be industry-accepted standards that are considered robust and reliable, and are consistent with Ohio IT Standard ITS-NET-01, "802.11 Wireless Local Area Network."

- 5.4.5. DAS/OIT/ISD Unified Network Services shall develop and implement a plan to manage radio frequencies and channels used by DAS' installed 802.11 technologies.

5.5 Network Management

- 5.5.1. DAS' facilities shall be scanned on a periodic and consistent basis by DAS/OIT/ISD Unified Network Services for the existence of unauthorized (rogue) 802.11 wireless network devices. DAS/OIT/ISD Unified Network Services shall report the existence of such devices to the DAS/OIT/ISD Deputy Director and shall immediately implement a plan to shut down, remove or confiscate any unauthorized 802.11 wireless device operating within DAS' facilities.
- 5.5.2. All DAS owned 802.11 wireless access points and client devices shall be audited on a consistent and on-going basis for intrusion prevention and detection by DAS/OIT/ISD Unified Network Services.
- 5.5.3. Use of the wireless network shall comply with DAS Policy; 700-01, Information Technology Resource Usage.

6.0 RELATED PROCEDURES

Standards and procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy. At a minimum:

- This policy shall be distributed to each newly hired DAS employee during orientation, in conjunction with other applicable policies, procedures, and standards; the new employee shall sign an acknowledgement of receipt of this policy.
- Vendors, contractors, and temporary employees shall receive a copy of and sign an acknowledgement of receipt of this policy prior to gaining access to IT resources.

7.0 COMPLIANCE

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

8.0 DEFINITIONS

Ad Hoc Mode - A wireless station (client) using 802.11 to communicate with another station in a peer-to-peer network configuration.

Anti-Virus Application Software - A commercially available computer program that detects, contains and eradicates malicious code.

DAS – Department of Administrative Services.

DAS Contractors – For the purposes of this policy, DAS contractors are defined as contracted staff and vendor technicians.

DAS Employees – For the purposes of this policy, DAS employees are defined as all employees and representatives of DAS, whether they are permanent staff or temporary staff.

DAS-owned – Purchased with DAS funds or otherwise acquired by DAS; property of DAS.

DAS-provided or DAS-supplied – Made available to users by DAS.

Encryption - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Enterprise Mode Pattern - A pattern that establishes a wireless network using enterprise-grade wireless access devices within the boundary of the agency network.

Hot Spot Mode Pattern - A pattern that establishes a wireless network allowing for personal-grade wireless devices as a separate perimeter, or sub-network, isolated outside the boundary of the agency network.

IT Resources – Any information technology resources, such as computer hardware and software, IT services, telecommunications equipment and services, networks, digital devices such as digital copiers and facsimile machines, supplies, and the Internet.

Management – Management refers to supervisory staff responsible for the completion of activities to fulfill DAS' mission. If Position A is shown as subordinate to Position B on the Table of Organization, then Position B is supervisory in nature for the purposes of this policy.

OIT – Office of Information Technology.

Patch - A procedure or software that corrects a malfunction or security vulnerability of a system.

Portable Computing Device - Computer or device designed for mobile use. Examples include laptops, personal digital assistants and mobile data collection devices.

Privately-owned - Purchased with personal or corporate (vendor or contractor) funds; not provided by the state.

State-owned - Purchased with state funds or otherwise acquired by the state; property of the state of Ohio.

Users - For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned IT Resources on behalf of the state.

Virtual Private Network (VPN) - A communications network tunneled through another network, typically for secure communications through an un-trusted or public network such as the Internet.

Wireless - Use of various electromagnetic spectrum frequencies, such as radio and infrared, to communicate services, such as data and voice, without relying on a hardwired connection, such as cable or fiber optics.

Wireless Access Point - A wireless network receiver and transmitter capable of connecting multiple wireless stations (clients) together using 802.11 to form a wireless local area network.

Wireless Device - Any device (including laptops, notebook personal computers, or desktops) with a wireless network interface card that can connect to the state's network.

9.0 RELATED RESOURCES

Document Name
ITA-NET-01, "802.11 Wireless Local Area Network Technical Architecture:" www.ohio.gov/itp
ITS-NET-01, "802.11 Wireless Local Area Network: Standard:" www.ohio.gov/itp
Wi-Fi Alliance Certification: http://certifications.wi-fi.org/wbcs_certified_products.php

10.0 INQUIRIES

For information regarding this policy, please contact:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, Suite 4083
Columbus, Ohio 43215
Telephone: 614.644.9391
Email: state.isp@oit.ohio.gov
Web: infosec.ohio.gov

Department of Administrative Services policies can be found online at:

<http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx>

11.0 REVISION HISTORY

Date	Description
12/01/2009	New policy for DAS, replaces OIT policy dated 11/02/07
12/05/2012	Policy reissued under Director Robert Blair.

12.0 ATTACHMENTS

None.