Wireless Local Area Network Policy

<table>
<thead>
<tr>
<th>POLICY NUMBER:</th>
<th>EFFECTIVE DATE:</th>
<th>APPOINTING AUTHORITY APPROVAL:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2100-06</td>
<td>12/21/2018</td>
<td></td>
</tr>
</tbody>
</table>

REPLACES POLICY DATED: 12/05/2012


1.0 PURPOSE

This policy addresses the use, management, and control of IEEE 802.11 wireless local area network (WLAN) protocols, commonly referred to as “wireless” within the Ohio Department of Administrative Services (DAS). These protocols are used for connecting client devices to a data network through the use of over-the-air radio signals. This policy also defines the permitted and prohibited uses of wireless services within DAS facilities or for DAS business use, including, but not limited to, both guest and private wireless networks.

A glossary of terms found in this policy is located in Section 8.0 Definitions. The first occurrence of a defined term is in bold italics.

2.0 SCOPE

This policy applies to all managers of DAS business units that are responsible for establishing or maintaining a DAS WLAN.

3.0 BACKGROUND

Wireless networks are the standard method for connecting to DAS networks. DAS offers wireless access via both guest and private networks. It is important to ensure security controls are in place to protect DAS wireless networks, the endpoints that connect to them, and the data that is transmitted or stored on the devices.

4.0 REFERENCES

4.1 Institute of Electrical and Electronics Engineers (IEEE): IEEE is a professional association that develops standards for wireless technology. The organization is considered an authority in a variety of areas, including aerospace systems,
computers and telecommunications, biomedical engineering, electric power and consumer electronics.

4.2 **Wi-Fi Alliance**: The Wi-Fi Alliance is a worldwide network of companies that develops Wi-Fi technology standards and certifies products to ensure they meet quality, performance, and security standards.

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 Administrative Policy IT-04, Use of Internet, E-mail, and Other IT Resources**: Ohio Administrative Policy IT-04 establishes controls on the use of state-provided IT resources to ensure that they are appropriately used for the purposes for which they were acquired.

4.5 **Ohio Administrative Policy IT-05, Disposal, Servicing and Transfer of IT Equipment**: Ohio Administrative Policy IT-05 mitigates risk with regard to state data, licensed software and intellectual property, and rechargeable batteries and other hazardous materials in the disposal, servicing or transfer of state agency IT equipment.

4.6 **Ohio Administrative Policy IT-14, Data Encryption and Securing Sensitive Data**: Ohio Administrative Policy IT-14 in conjunction with Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," provides guidance to agencies as they take steps to protect sensitive data and information.

4.7 **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.

5.0 **POLICY**

All WLAN technologies authorized to connect to the state’s private network shall adhere to the following configuration, implementation and management requirements:

5.1 **Network Configuration**

5.1.1 Access to state network assets from state-owned wireless client devices shall be through wireless access points (WAPs) in infrastructure mode only. No ad hoc mode is permitted.
5.1.2 WAP 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). The guest network shall be outside the boundary of the internal network.

5.2 **Wireless Access Points (WAPs)**

5.2.1 All WAPs shall be requested and authorized by DAS Office of Information Technology (OIT) Unified Network Services (UNS). No unauthorized WAPs shall be connected to the state's network.

5.2.2 All WAPs shall be industry certified by the Wi-Fi Alliance to guarantee interoperability and enterprise-level security capabilities.

5.2.3 All WAPs shall be listed in a registry maintained by the state's wireless access provider.

5.2.4 All default WAP names, usernames and administrator passwords shall be changed prior to installation.

5.2.5 All WAPs shall be named in a manner consistent with the naming convention developed and managed by DAS OIT UNS.

5.2.6 WAPs shall include a broadcast identifier, SSID, in a format approved by DAS OIT UNS.

5.2.7 All WAPs, included in the state's asset inventory, that are taken out of service shall be disposed of by DAS OIT UNS, as outlined in Ohio Administrative Policy IT-05, "Disposal, Servicing and Transfer of IT Equipment."

5.2.7.1 DAS OIT UNS shall ensure the removal of WAP configuration information, such as passwords; keys; names; network addresses; and other pertinent information, prior to disposal.

5.2.7.2 WAPs removed by the state's **service provider** are not state assets; are not capable of retaining configuration information; and are therefore, not subject to the disposal rules outlined in Ohio Administrative Policy IT-05.
5.3 Wireless Client Devices

5.3.1 All state-owned and state-authorized wireless client devices shall be Wi-Fi Alliance certified to guarantee interoperability and enterprise-level security capabilities.

5.3.2 DAS OIT UNS shall implement controls to ensure that wireless client devices authorized to connect to DAS networks, whether wireless or wired networks, are configured to prevent connections from or to other wireless client devices in ad-hoc or peer-to-peer mode.

5.3.3 DAS OIT UNS shall implement controls to ensure that portable devices authorized to connect to DAS private wireless networks have personal firewalls, up-to-date antivirus definitions (when applicable), and security patches.

5.4 Network Operations

5.4.1 The wireless 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 WLAN, that is considered sensitive data, shall be encrypted in a manner consistent with Ohio Administrative Policy IT-14, "Data Encryption and Securing Sensitive Data."

5.4.3 Access to the DAS wireless network for state business or access to sensitive information shall include client device and end-user authentication.

5.4.4 Authentication mechanisms or protocols selected shall be industry-accepted standards that are considered robust and reliable.

5.4.5 The DAS OIT service provider shall develop and implement a plan to manage radio frequencies and channels used by DAS’ installed wireless technologies.

5.5 Network Management

5.5.1 DAS wireless networks shall be routinely scanned for rogue devices. The DAS Office of Information Security and Privacy (OISP) Security Monitoring team shall be notified when rogue devices are identified.
5.5.2 The DAS OISP Security Monitoring team shall be responsible for planning the shutdown, removal, or confiscation of unauthorized wireless devices operating within DAS facilities.

5.5.3 All WAPs and client devices shall be audited on a consistent and on-going basis for intrusion prevention and detection by DAS OIT UNS.

5.5.4 All WAPs shall be configured to send audit log information to the enterprise security information and event management (SIEM) solution.

5.5.5 Use of the DAS wireless network shall comply with DAS Policy 700-01, "Information Technology Resource Usage.

6.0 PROCEDURES

None.

7.0 COMPLIANCE

To assist DAS entities with meeting the WLAN requirements outlined in the policy, a general implementation framework includes:

7.1 For existing wireless LANs, WAPs, and wireless client devices, the requirements shall be implemented within six months from the effective date of the policy.

7.2 All planned and future wireless LAN, WAP, or wireless client device implementations shall immediately comply with the requirements outlined in this policy.

8.0 DEFINITIONS

Ad Hoc Mode - This is a wireless network configuration that does not use access points; stations communicate directly with each other. ¹

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.

**Firewall** - A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. ²

**Infrastructure Mode** – This wireless network configuration requires access points and is the most commonly used mode for WLANs. All stations connect with an access point, and the access point transfers frames among the stations and the distribution system. ³

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

**Peer-to-Peer Mode** – See definition for *ad hoc mode*.

**Personally Identifiable Information** - “Personally identifiable information” (PII) is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

**Portable Devices** - Computer or device designed for mobile use. For the purposes of this policy, a portable device includes laptops, smartphones or tablets.

**Service Provider** – For the purposes of this policy, the service provider is the vendor with whom DAS contracts to provide wireless local area network support (e.g., design, implementation, and management).

DAS OIT is also considered a WLAN service provider to other state agencies, boards, and commissions.

**Sensitive Data** - Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially


a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, Criminal Justice Information under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy, and the Social Security Administration Limited Access Death Master File. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

**Station** - A station is a wireless endpoint device, such as a laptop or mobile phone. (Technically, a station is a wireless network interface implementation. It is distinct from the device that will provide an application using the network interface (such as a laptop or mobile phone).  

**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 (e.g., laptops, or desktops) with a wireless network interface card that can connect to the state's network.

**9.0 INQUIRIES**

Direct inquiries about this policy to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor
Columbus, Ohio 43215

---

10.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/01/2009</td>
<td>New policy for DAS, replaces OIT policy dated 11/02/07.</td>
</tr>
<tr>
<td>12/05/2012</td>
<td>Policy reissued under Director Robert Blair</td>
</tr>
<tr>
<td>12/21/2018</td>
<td>Updated the policy to align with current technology and DAS OIT’s approach to the management of wireless services.</td>
</tr>
<tr>
<td>06/10/2020</td>
<td>Updated the policy template to align with the current format.</td>
</tr>
<tr>
<td>06/10/2021</td>
<td>Scheduled policy review.</td>
</tr>
</tbody>
</table>

11.0 ATTACHMENTS

None.