



KAY IVEY
Governor

STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



MARTY REDDEN
Acting Secretary

POLICY 637: Wireless Security

VERSION NUMBER	Policy 637-01
VERSION DATE	July 30, 2019
POLICY TITLE	Wireless Security
OBJECTIVE	The objective of this policy is to establish security roles and responsibilities for implementing and operating a wireless local area network (WLAN) and wireless devices within the state information network.
AUTHORITY	<p>The authority of the Office of Information Technology (OIT) to create and enforce policies relating to the management and operation of information technology (IT) by state agencies, and exceptions to such authority, are derived from:</p> <p><i>Articles 8 and 11 of Chapter 4 of Title 41, and Chapter 28 of Title 41, Code of Alabama 1975 (Acts 2013-68 and 2017-282).</i></p> <p>Policies of OIT are approved and signed by the Governor.</p>
APPLICABILITY	The requirements and responsibilities defined in OIT policies apply to all departments, agencies, offices, boards, commissions, bureaus, and authorities (referred to generally as agency or agencies) and authorized individuals in the employment of the State of Alabama responsible for the management, operation, or use of state IT.
STATEMENT OF POLICY	<p>It is the policy of OIT that:</p> <ol style="list-style-type: none"> a) All WLAN components shall use Federal Information Processing Standard (FIPS) 140-2 compliant cryptographic algorithms to protect the confidentiality and integrity of WLAN communications. [AC-18 a.] b) Agencies operating a legacy 802.11 WLAN shall have a plan in place to upgrade their WLAN to 802.11i for FIPS compliance by year 2020 (if financially feasible). [AC-18 a.]

- c) WLAN devices shall comply with state WLAN security configuration policies and standards. [AC-18 a.]

OIT
RESPONSIBILITIES

OIT shall:

- O.1 Perform both attack monitoring and vulnerability scanning to support WLAN security of the state network. [SI-4 a.]
- O.2 Centrally manage WLAN access points (APs) for agencies within the OIT network address space to promote standardized wireless security posture. [AC-18 b.]
- O.3 Coordinate with agencies planning to implement WLANs to ensure security requirements meet state standards. [CM-2 (1)]
- O.4 Conduct annual technical security assessments of WLANs operating in the OIT network address space. [CA-1 b.2.]

AGENCY
RESPONSIBILITIES

Agencies shall:

- A.1 Agencies operating outside of the OIT domain shall provide a security plan to the State Cybersecurity Council for approval prior to obtaining or deploying a WLAN. [SC-1 a.1., a.2.]
- A.2 Require users of approved wireless mobile devices to authenticate with state computer logon credentials prior to allowing access to state information resources. [AC-18 (CE1)]
- A.3 Require wireless mobile devices to authenticate before establishing a network connection to information resources. [AC-18 (CE1)]
- A.4 Ensure only approved WLANs in compliance with state standards are allowed to connect with the state information network unless granted a waiver by the OIT. [AC-18 b.]
- A.5 Utilize standard security configurations for WLAN devices (e.g., laptops, smart phones, tablets, and wireless access points). [CM-6 a.]
- A.6 Develop and implement a physical and environmental protection plan for agency wireless access points to protect against tampering or theft. [PE-3]
- A.7 Perform annual technical security assessments of agency WLAN. [CA-1 b.2.]
- A.8 Disable dual connection option on mobile wireless (i.e., Wi-Fi and wired connection or wired connection and Bluetooth) devices accessing state information resources to reduce system attack surface. [AC-18 (CE3)]

**USER
RESPONSIBILITIES**

Users shall NOT:

U.1 Attempt to circumvent WLAN security policies, standards, procedures. [PL-4 a.]

U.2 Utilize unapproved wireless mobile devices to access state information networks. [PL-4 a.]

**SUPPORTING
DOCUMENTS**

The following documents support this policy:

- [Standard 637S1: Wireless Networks](#)
- [Standard 637S2: Wireless Clients](#)
- [Standard 637S3: Bluetooth Security](#)

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support this policy and may aid in its implementation:

- NIST SP 800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
- NIST SP 800-121R2: Guide to Bluetooth Security
- NIST SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)

EFFECTIVE DATE

This policy shall be effective upon its approval by the Secretary of Information Technology and the Governor of Alabama as evidenced by the signatures of the Secretary and Governor being affixed hereto.

SUPERSEDES

This policy supersedes legacy Policy 643: Wireless Security, which is hereby rescinded.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this policy to be adopted as of the date on which the Governor has approved and signed it.

Marty Redden
Acting Secretary of Information Technology

ORDERED

Kay Ivey
Governor

This _____ day of _____, 2019.

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
637-01	07/30/2019	Initial version