



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 637S1: Wireless Networks

VERSION NUMBER	Standard 637S1-01
VERSION DATE	July 30, 2019
STANDARD TITLE	Wireless Networks
GOVERNING POLICY	This standard is governed by Policy 637: Wireless Security, regardless of revision.
OBJECTIVE	Ensure all organizations deploy, manage, and/or utilize wireless technologies with an acceptable level of security
REQUIREMENTS	<p>Based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-48: Wireless Network Security, and NIST Special Publication 800-97: Guide to IEEE 802.11i: Establishing Robust Security Networks, State of Alabama organizations that deploy, manage, or utilize wireless networks shall comply with the following requirements:</p> <ol style="list-style-type: none">1. INITIATION<ol style="list-style-type: none">1.1. Undertake wireless network deployment for operations only after conducting a thorough risk assessment to understand wireless local area network (WLAN) threats, the likelihood those threats will be realized, and the potential impact of realized threats on the value of the organization's assets. [RA-3]1.2. The authentication server (AS) should be among the most secure servers in the enterprise because a breach of an AS could allow an adversary to access the network without a physical connection, perhaps even beyond the organization's physical perimeter, therefore, AS operating system and application security configuration must meet or exceed state standards for server security. [CM-6]

- 1.3. Administration and network management of WLAN infrastructure equipment requires strong authentication and encryption of all communication. If an organization uses Simple Network Management Protocol (SNMP) to manage its equipment, it must use SNMP version 3. [IA-3 (CE4)]
- 1.4. Use SSL/TLS or an equivalent protection (e.g., IPSec VPN) for Web-based administration. [IA-7]
- 1.5. Promote awareness of the technical and security implications of wireless technology. This may be accomplished through annual security awareness education. [AT-2]

2. PLANNING AND DESIGN

- 2.1. Conduct a site survey to determine the proper location of wireless access points (APs), given a desired coverage area. The site survey shall result in a report that proposes the location for each AP, graphically notes its usable coverage area, and assigns it an IEEE 802.11 radio channel. The estimated usable range of each AP should not extend beyond the physical boundaries of the facility unless required. Place APs in secured areas to prevent unauthorized physical access and user manipulation. Position APs away from exterior walls and windows; use interior walls or position near the center of the room if possible. After deployment, test AP range boundaries to determine the precise extent of wireless coverage. Include survey results in site security plans. [AC-18 (CE5)]
- 2.2. Create a dedicated Virtual LAN (VLAN) to support AP connections to the distribution system (e.g., enterprise wired network) and ensure that network management information between APs/ASs and network management servers or console is transmitted over a dedicated management VLAN. [AC-18]
- 2.3. APs and ASs shall send event data to a secure audit server in real time so that the integrity of previously captured audit data is protected even when the AP or AS is compromised.
 - 2.3.1. Events to be captured shall include, at a minimum, both successful and unsuccessful authentication and association attempts.
 - 2.3.2. Store audit records in accordance with applicable state or federal standards. [AU-11]
- 2.4. Utilize the Protected Extensible Authentication Protocol (PEAP) method for WLAN authentication. [IA-3]

- 2.5. Document the fallback procedure for when WLAN authentication fails. This may involve:
 - Calling the help desk to reset a password.
 - Verifying user identification and authorization.
 - Installing client certificate if necessary. [SI-11]
- 2.6. Deploy wireless intrusion detection systems to detect suspicious or unauthorized activity. The radio coverage of wireless intrusion detection devices should be at least as great as that of the WLAN they are intended to protect. [CA-7]

3. PROCUREMENT

- 3.1. The Wi-Fi Alliance industry group certifies WLAN products as meeting specific standards. When a WLAN product is marked as Wi-Fi compliant, the product was evaluated by the Wi-Fi Alliance laboratory and meets the requirements found in the IEEE 802.11a, b, or g standards. Products certified as Wi-Fi WPA2 implement the requirements of the IEEE 802.11i specification.
- 3.2. Procure only WPA2-Enterprise certified devices and AP products. Only WPA2-Enterprise certified products are capable of fully implementing the IEEE 802.11i Robust Security Network (RSN) protections. [AC-18]
- 3.3. Procure products that use Federal Information Processing Standard (FIPS)-validated cryptographic modules. [IA-7]
- 3.4. Procure devices and APs that support NIST AES key wrap with 128-bit HMAC-SHA-1 to protect transient keys during the 4-Way and Group Key Handshakes. [AC-18]
- 3.5. Procure ASs and APs that communicate in a secure manner. [AC-18]
- 3.6. Procure products that support PEAP. Test interoperability between devices and ASs before final procurement. [AC-18 (CE1)]
- 3.7. Procure APs and ASs that terminate associations after a configurable time period. [AC-12]
- 3.8. Procure APs that log security relevant events and forward them to a remote audit server in real time. The AP shall support the functional audit requirements in applicable state standards. [AU-6]

- 3.9. Procure APs that can support an independent management interface to the distribution system (e.g., wired network). An independent management interface enables maintainers to utilize an out of band channel for key transfer and other administrative functions. [AC-18]
- 3.10. Procure APs that support SNMPv3 if the organization plans SNMP-based AP management. [AC-18]
- 3.11. Procure APs that support authentication and data encryption for administrative sessions (e.g., SSL/TLS support for Web-based administration and secure shell (SSH) for command-line administration). [AC-18 (CE1)]
- 3.12. Procure client devices whose software can be configured to specify valid ASs by name. [AC-18]
- 3.13. Procure APs and ASs that support IPsec or alternative security methods to establish a mutually authenticated secure communications channel between AP and AS. [AC-18 (CE1)]
- 3.14. Procure APs and ASs that support Network Time Protocol (NTP). The nonce in the 4-way handshake shall be based on NTP time whenever possible. NTP allows distributed devices to synchronize timestamps, which is critical to effective log analysis. [AC-18]
- 3.15. Procure products that can be upgraded easily in software or firmware so they can take advantage of wireless security patches and enhancements released after original delivery. [SA-4 (CE5)]
- 3.16. Organizations planning to deploy a product not meeting the above standards shall submit a security plan to the Office of Information Technology (OIT) for analysis and approval. [CA-2]

4. IMPLEMENTATION

- 4.1. Disable all insecure and unused management protocols (e.g., SNMPv1 and SNMPv2) on the APs, and configure remaining management protocols for least privilege (i.e., read only) unless write access is required (e.g., to change configuration settings as part of an automated incident response procedure). Disable SNMP if it is not used. [CM-7 (CE1)]
- 4.2. Ensure all APs use strong, unique administrative passwords. [CM-5 (CE1)]
- 4.3. Disable WEP and all other unused protocols in the configuration of each AP. [CM-7 (CE1)]

4.4. Activate logging, direct log entries to a remote audit server, and review logs in accordance with state log management standards. [AU-2] [AU-12]

5. OPERATIONS AND MAINTENANCE

5.1. Enforce user authentication at the wireless access point before granting access to state network resources. All implementations must support and employ strong user authentication which checks against an external database such as RADIUS or Kerberos. [AC-18 (CE1)]

5.2. Implement two-factor authentication for administrative connections to the WLAN infrastructure. [IA-2 (CE1)]

5.3. Proactively search reports on newly discovered wireless threats and vulnerabilities. Newly discovered security vulnerabilities of vendor products must be handled in accordance with state vulnerability management programs. [RA-3]

5.4. Ensure passwords are being changed in accordance with state standards. [IA-5 (CE1)]

5.5. Maintain a complete inventory of all WLAN components, especially APs. A complete inventory of an organization's authorized APs is the basis for identifying rogue APs during security audits. [CM-8 (CE1, 3)]

5.6. Perform comprehensive WLAN security assessments semi-annually. WLAN security assessments shall include verification of device, AP and AS configuration settings, review of audit logs, and radio detection of rogue APs. Scan monthly for rogue APs. [CA-2] [CA-2 (CE2)]

5.7. User authentication mechanisms shall be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP. [AC-5] [AC-6 (CE1, 5)]

5.8. Ensure that management traffic destined for APs is on a dedicated wired subnet or management VLAN. [SA-8] [AC-18]

5.9. When practical, use a local serial port interface for AP configuration to minimize the exposure of sensitive management information. [MA-3 (CE1)]

5.10. Authorized personnel shall restore an AP to its proper security configuration following a reset. Security settings typically are returned to factory defaults after a reset event. [CM-2 (CE1)] [AC-5]

6. DISPOSITION

6.1. When disposing of a WLAN component, remove all sensitive data and configuration information. [MP-6]

- Use degauss devices when feasible,
- Disk wiping utilities can be used for devices that have hard disks, or
- Clear configuration settings manually using the management interface.

6.2. When disposing of a WLAN component, ensure that its audit records are retained as needed to meet regulatory or agency information retention requirements. [AU-11]

7. AP AUTHORIZATION AND AUDIT

7.1. Wireless APs connected to any state network shall be authorized by the network owner. APs that are not authorized shall be removed from service immediately. [CA-6]

7.2. APs are subject to periodic vulnerability scanning in accordance with state or agency risk assessment policy, vulnerability scanning procedures, and other applicable requirements or standards. [RA-5]

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 637: Wireless Security](#)
- [Standard 637S2: Wireless Clients](#)

The following special publications (SP) of the National Institute of Standards and Technology (NIST) support these requirements and may aid in their implementation:

- NIST SP 800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
- NIST SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)

EFFECTIVE DATE

This standard is effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

SUPERSEDES

This standard supersedes legacy Standard 643S1: Wireless Networks, 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 standard to be adopted as of the _____ day of _____, 2019.

Marty Redden
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
637S1-01	07/30/2019	Initial version