



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 637S2: Wireless Clients

VERSION NUMBER	Standard 637S2-01
VERSION DATE	July 30, 2019
STANDARD TITLE	Wireless Clients
GOVERNING POLICY	This standard is governed by Policy 637: Wireless Security, regardless of revision.
OBJECTIVE	Ensure organizations and individuals deploy, manage, and 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 agencies that deploy, manage, or utilize wireless networks shall comply with the following requirements:</p> <ol style="list-style-type: none">1. CLIENT DEVICE SECURITY<ol style="list-style-type: none">1.1. Only Federal Information Processing Standard (FIPS) validated 802.11i solutions using IEEE 802.1X/EAP authentication (rather than pre-shared keys) are approved for use on state networks. Legacy wireless clients that do not support 802.11i and WPA-2 must utilize a state-approved Virtual Private Network (VPN) solution configured in accordance with applicable state standards. [AC-18]1.2. Ensure that client devices connecting directly to a state network connect only to a valid authentication server (AS). To ensure authorized connections, the device should be configured to specify the names of valid ASs, specify the locally stored certification authority (CA) certificate used to validate the digital signature of the AS certificate, and require that the device check for AS certificate revocation. [AC-18]1.3. Disable ad hoc mode on wireless devices. [CM-7]

- 1.4. Turn off communication ports (if possible) during periods of inactivity to minimize the risk of malicious access. [CM-7]
- 1.5. Ensure desktop application mirroring software is password protected. [CM-6]
- 1.6. Wireless devices must undergo security assessments to identify security vulnerabilities. [CA-2 (CE1)]
- 1.7. Ensure physical security of wireless devices in accordance with physical security standards and applicable system (laptop, smart phones, tablets, etc.) security standards. [PE-3]
- 1.8. Ensure wireless devices are configured in accordance with applicable system (laptop, smart phones, tablets, etc.) security standards or baselines. [AC-18]
- 1.9. Wireless access and authentication must comply with network and system access policies and standards (i.e., password standards, lock-out settings, session time-out, etc.). [AC-18] [AC-12] [IA-5]
- 1.10. Prior to disposing of a wireless device, ensure the device has been properly sanitized in accordance with media sanitization standards. [MP-6]

2. MOBILE DEVICE SECURITY

Security configuration and access controls for wireless mobile devices are addressed in [Policy 638: Mobile Device Access Control](#) and mobile device standards and procedures.

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 637: Wireless Security](#)
- [Standard 637S1: Wireless Networks](#)

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 643S2: Wireless Clients, 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
637S2-01	07/30/2019	Initial version