STATE OF ALABAMA

Information Technology Standard

STANDARD 643S2-00: WIRELESS CLIENTS

WLAN-capable devices typically are at greater risk of a security breach than wired-only devices and may require additional security controls beyond those already present. This standard describes how wireless client devices are to be deployed, managed and utilized by State of Alabama organizations. These requirements apply to wireless-capable laptop PCs, personal digital assistants (PDA), text-messaging devices and smart phone-PDA products.

OBJECTIVE:

Ensure all organizations deploy, manage, and/or utilize wireless technologies with an acceptable level of security.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

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.

- Only 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 shall utilize a State-approved Virtual Private Network (VPN) solution configured in accordance with applicable State standards.
- Ensure that the client devices connecting directly to the 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.
- Disable ad hoc mode on wireless devices.
- Turn off communication ports (if possible) during periods of inactivity to minimize the risk of malicious access.
- Synchronize devices with their corresponding PCs regularly to ensure data availability.
- Ensure desktop application mirroring software is password protected.
- Wireless devices shall undergo security assessments to identify security vulnerabilities.
- Ensure physical security of wireless devices in accordance with physical security standards and applicable system (laptop, PDA, etc.) security standards.
- Ensure wireless devices are configured in accordance with applicable system (laptop, PDA, etc.) security standards and/or baselines.
- Wireless access and authentication shall comply with network and system access policies and standards (i.e., password standards, lock-out settings, session time-out, etc).
- Prior to disposing of a wireless device, ensure the device has been properly sanitized in accordance with state media sanitization standards.

SUPPORTING DOCUMENTS:

- Information Technology Policy 643: Wireless Security
- Information Technology Standard 643S1: Wireless Networks
- Information Technology Standard 643S3: Bluetooth Security

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
643S2-00	09/01/2011	Replaces Standard 640-03S2 (format and number change only)