STATE OF ALABAMA

Information Technology Standard

STANDARD 643S3-00: BLUETOOTH SECURITY

Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, digital cameras and video game consoles via a secure, globally unlicensed short-range radio frequency

OBJECTIVE:

Ensure all organizations deploy and/or utilize Bluetooth 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, State of Alabama organizations that deploy and/or manage Bluetooth technologies shall comply with the following requirements:

MANAGEMENT CONTROLS

Promote awareness of the technical and security implications of Bluetooth technology.

Undertake wireless network deployment for operations only after conducting a thorough risk assessment and defining a risk mitigation plan.

Perform comprehensive security assessments semi-annually to validate the secure configuration of Bluetooth technology and to fully understand the wireless security posture.

Make sure the wireless “network” is fully understood. With piconets forming scatter-nets with possible connections to 802.11 networks and connections to both wired and wireless wide area networks, an agency must understand the overall connectivity.

Make sure that handheld and small Bluetooth devices are protected from theft.

Shut down Bluetooth devices when not in use to minimize exposure to potential malicious activities.

Maintain a complete inventory of all Bluetooth-enabled wireless devices.

Study and understand all planned Bluetooth-enabled devices to understand the security implications. An understanding of the security implications of Bluetooth will help the organization better address the associated risks.

TECHNICAL CONTROLS

Change the default settings of the Bluetooth device to reflect the agency’s security policy.

Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the agency.

Ensure that the Bluetooth “bonding” environment is secure from eavesdroppers (i.e., the environment has been visually inspected for possible adversaries before the initialization procedures during which key exchanges occur).

Choose PIN codes that are sufficiently random and avoid all weak PINs.

Choose PIN codes that are sufficiently long (maximum length possible).

Ensure that no Bluetooth device defaults to the zero PIN.

Configure Bluetooth devices to delete PINs after initialization, to ensure that PIN entry is required every time and that PINs are not stored in memory after power removal to prevent the possibility of a PIN being recovered from the memory of a stolen device.

OPERATIONAL CONTROLS

Ensure that combination keys are used instead of unit keys.

Link encryption shall be used to secure all data transmissions during a Bluetooth connection.

Ensure that encryption is enabled on every link in the communication chain.

Ensure device mutual authentication for all accesses.

Enable encryption for all broadcast transmissions (Encryption Mode 3).

Configure encryption key sizes to the maximum allowable.

Ensure that portable devices with Bluetooth interfaces are configured with passwords to prevent unauthorized access if lost or stolen.

State-approved antivirus software shall be installed on Bluetooth-enabled hosts.

Newly discovered security vulnerabilities of vendor products shall be patched to prevent malicious and inadvertent exploits. Patches shall be fully tested before implementation.

Whenever possible, implement strong user authentication mechanisms (such as two-factor authentication, biometrics, smart cards, or PKI) to minimize the vulnerabilities associated with passwords and PINs.

Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.

Organizations shall fully understand the technical, security, operational, and personnel requirements before implementation of any security feature or product.

Proactively search reports on newly discovered Bluetooth threats and vulnerabilities.

SUPPORTING DOCUMENTS:

- Information Technology Policy 643: Wireless Security
- Information Technology Standard 643S1: Wireless Networks
- Information Technology Standard 643S2: Wireless Clients

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

DOCUMENT HISTORY:

Version	Release Date	Comments
643S3-00	09/01/2011	Replaces Standard 640-03S3 (format and number change only)