Bluetooth Baseline Requirements Policy

1.0 Purpose

The proliferation of Bluetooth-enabled devices presents potential security risks if connections are not properly secured. Insecure Bluetooth usage can expose organizational devices and networks to unauthorized access, data leakage, or malware introduction. The purpose of this standard is to establish minimum security requirements for the use of Bluetooth technology with organization-owned devices or when connecting to the organization's network, ensuring sufficient protection for organizational data, including Personally Identifiable Information (PII) and other confidential information.

2.0 Scope

This standard applies to all employees, contractors, vendors, and other personnel utilizing any Bluetooth-enabled device (whether organization-owned or personal) that connects to organization-owned equipment (e.g., laptops, mobile phones) or directly interacts with the organization's network infrastructure.

3.0 Policy Statements

The following minimum standards must be adhered to when using Bluetooth technology in conjunction with organizational resources:

3.1 Approved Bluetooth Versions

* Unless a formal exception is granted in advance by the designated IT authority (e.g., Precision Computer Team), only Bluetooth devices meeting the Bluetooth Core Specification version 2.1 + EDR (Enhanced Data Rate) or higher are permitted for use with organization equipment or networks.
* Devices purchased prior to the implementation date of this standard may be exempt from the minimum version requirement but must comply with all other aspects of this standard. However, upgrading legacy devices is strongly encouraged.

3.2 Secure Pairing Procedures

* **Pairing Location:** Initial pairing of Bluetooth devices (establishing a trusted connection) should only be performed in a private, secure location to prevent unauthorized observation or interception of pairing codes (PINs) or processes. Avoid pairing devices in public areas.

*   **PIN Security:** Use strong, non-default PINs for pairing whenever possible. Do not use easily guessable PINs like "0000" or "1234".
*   **Unsolicited Pairing Requests:** If a device prompts for pairing or requests a PIN unexpectedly after the initial secure pairing has been completed, *do not* accept the request. This could indicate an attempted security compromise. Report such incidents immediately to the IT Help Desk for investigation by the designated IT authority (e.g., Precision Computer Team).

3.3 Discoverability (Visibility)

*   Bluetooth devices should be set to "non-discoverable" or "hidden" mode whenever Bluetooth functionality is not actively needed for pairing or connection establishment. This limits the ability of unauthorized devices to detect their presence.

3.4 Unused Connections

*   Disable Bluetooth functionality on organizational devices when it is not actively required for business purposes to reduce the potential attack surface.
*   Regularly review the list of paired devices on organizational equipment and remove any devices that are no longer needed or recognized.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer Team) may verify compliance with this standard through various methods, including device configuration audits, security scans (where feasible), and investigation of reported incidents.

4.2 Exceptions

Any exception to this standard (e.g., use of older Bluetooth versions for specific legacy equipment) requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer Team).

4.3 Enforcement

Failure to comply with this standard may result in the disabling of Bluetooth functionality on organizational devices or other corrective actions. Violations may also lead to disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Definitions

*   **Bluetooth:** A short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances.
*   **Pairing:** The process of establishing a trusted, authenticated connection between two Bluetooth devices, often involving the exchange or confirmation of a PIN.
*   **PIN (Personal Identification Number):** A numeric or alphanumeric code used in some

Bluetooth pairing processes for authentication.
* **Discoverable Mode:** A Bluetooth setting that allows a device to be detected by other nearby Bluetooth devices scanning for connections.

Revision #2
Created 28 August 2024 16:49:05 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery