Wireless Communication Standard

1.0 Purpose

This standard defines the minimum technical requirements that wireless infrastructure devices (e.g., access points, routers) must meet to be authorized for connection to the organization's network. The objective is to ensure the security and integrity of the network by controlling wireless access and mitigating associated risks. Only devices meeting these standards, or those granted a formal exception, are permitted.

2.0 Scope

This standard applies to all employees, contractors, consultants, temporary staff, and other personnel of the organization and its subsidiaries. It covers any individual who installs, manages, or utilizes wireless infrastructure devices that connect to, or provide connectivity to, the organization's network infrastructure. This includes both corporate-managed and user-managed (e.g., home) wireless devices used for accessing organizational resources.

3.0 Policy Statements

The following technical standards and requirements apply to all wireless infrastructure devices connecting to the organization's network:

3.1 General Requirements for Corporate Wireless Devices

All wireless infrastructure devices managed by the organization or connecting directly to the corporate network infrastructure, particularly those providing access to Confidential, Highly Confidential, or Restricted information (as defined by the organization's Data Classification Policy), must adhere to the following minimum security configurations:

*   **(Placeholder: Specific requirements need to be detailed here.** Examples might include: WPA2/WPA3 Enterprise authentication, specific EAP types like EAP-TLS or PEAP, disabling SSID broadcast for certain networks, strong administrative credentials, regular firmware updates, physical security considerations, prohibition of open/guest networks without proper segmentation, etc.)

3.2 Requirements for Home/Remote Wireless Devices Accessing Corporate Network

Wireless infrastructure devices located in remote or home environments that provide direct access to the organization's internal network (e.g., supporting hardware VPN connections or specific

teleworker solutions) must meet the following minimum security standards:

* **(Placeholder: Specific requirements need to be detailed here.** Examples might include: WPA2/WPA3 Personal (PSK) with strong, complex passphrases, changing default administrative credentials, enabling network encryption, disabling UPnP, keeping firmware updated, ensuring the device is physically secure, etc.)

3.3 Approval and Exceptions

Only wireless infrastructure devices that meet the requirements specified in this standard are approved for connectivity. Any exception must be formally documented, justified, and approved in advance by the designated IT authority (e.g., Precision Computer Team).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer Team) will verify compliance with this standard through various methods, including but not limited to network scanning, device configuration audits, log reviews, physical inspections, and analysis of security tool reports. Findings will be reported to the policy owner and relevant management.

4.2 Exceptions

As stated in section 3.3, any exception to this standard 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 disconnection of non-compliant devices from the network. Violations by personnel may lead to disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Definitions

For clarity, the following terms are relevant to this standard. Further definitions can often be found in established industry security glossaries:

* **AES (Advanced Encryption Standard):** A strong symmetric block cipher algorithm used for data encryption.
* **EAP (Extensible Authentication Protocol):** An authentication framework often used in wireless networks (e.g., EAP-FAST, EAP-TLS, PEAP).
    * **EAP-FAST (Flexible Authentication via Secure Tunneling)**
    * **EAP-TLS (Transport Layer Security)**
    * **PEAP (Protected Extensible Authentication Protocol)**
* **SSID (Service Set Identifier):** A name that identifies a wireless network.
* **TKIP (Temporal Key Integrity Protocol):** An older encryption protocol used with WPA; now considered less secure than AES.

*   **WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key):** A security protocol using a shared key for authentication, commonly used in home networks (also known as WPA/WPA2/WPA3 Personal).

Revision #2
Created 28 August 2024 16:45:55 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery