Wireless Communication Policy

1.0 Purpose

Wireless networking (Wi-Fi) is prevalent and essential for connectivity using devices like laptops, smartphones, and tablets. However, insecure wireless configurations create significant vulnerabilities that malicious actors can exploit. The purpose of this policy is to establish the minimum security requirements for deploying, configuring, and connecting wireless infrastructure devices (access points, routers) and client devices to the organization's network. This policy aims to protect the confidentiality, integrity, and availability of the organization's information assets by managing the risks associated with wireless technologies.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, and other personnel ("Users") at the organization, including affiliates and third parties who manage or use wireless infrastructure or connect devices wirelessly to the organization's network. It covers all wireless infrastructure devices operating on organizational sites or connecting to the network, and all devices (laptops, desktops, mobile phones, tablets, IoT devices, etc.) using wireless communications to access organizational resources. This includes any form of wireless communication capable of transmitting packet data.

3.0 Policy Statements

Access to the organization's network via wireless technology is a privilege conditioned on adherence to the following security requirements:

3.1 General Requirements for Corporate Wireless Networks

All wireless infrastructure devices deployed within organizational facilities that connect to the primary corporate network, or provide access to information classified as Confidential or higher (per the Data Classification Policy), must adhere to the following minimum security standards:

*   **Authentication:** Must utilize strong, enterprise-grade authentication protocols (e.g., WPA2-Enterprise or WPA3-Enterprise using EAP-TLS, PEAP, or other approved EAP types) integrated with the organization's central authentication system (e.g., RADIUS, Active Directory). Pre-shared keys (PSK) are prohibited for primary corporate network access.
*   **Encryption:** Must use strong encryption algorithms (e.g., AES/CCMP). Deprecated protocols like WEP or WPA/TKIP are prohibited.

*   **SSID Management:** Service Set Identifiers (SSIDs) for corporate access must not be broadcast where feasible or required by specific security directives. Guest network SSIDs may be broadcast but must be segregated. Default SSIDs must be changed.
*   **Device Management:** Access points must be centrally managed using organization-approved systems. Default administrative credentials must be changed immediately upon deployment using strong, unique passwords compliant with the Password Policy. Firmware must be kept up-to-date with security patches.
*   **Network Segmentation:** Corporate wireless networks must be appropriately segmented from guest or other less trusted networks using VLANs and firewall rules.
*   **Rogue AP Detection:** Mechanisms must be in place to detect and mitigate unauthorized (rogue) wireless access points connected to the corporate network.
*   **(Placeholder: Add any other specific requirements, e.g., specific configuration settings, physical security of APs).**

3.2 Requirements for Laboratory or Isolated Wireless Networks

Wireless networks deployed in laboratory or other isolated environments that **do** provide access to Confidential or higher organizational data must adhere to the requirements in section 3.1.

Wireless networks within labs or isolated environments that **do not** provide general connectivity to the corporate production network must still meet the following minimum requirements:

*   **Authentication & Encryption:** Must utilize, at minimum, WPA2/WPA3 Personal (PSK) with strong, complex passphrases compliant with the Password Policy. Open (unencrypted/unauthenticated) wireless networks are strictly prohibited if handling any organizational data or connected to any equipment processing such data.
*   **Network Isolation:** Must be demonstrably segregated from the corporate production network (e.g., via air gap or dedicated firewalls configured according to organizational standards). Any connection between lab/isolated networks and the corporate network requires explicit approval and security review by the designated IT authority (e.g., Precision Computer team, Lab Security Group).
*   **Device Management:** Default administrative credentials must be changed. Firmware should be kept updated.
*   **(Placeholder: Add any other specific lab/isolated requirements).** Adherence to specific Lab Security Policies is also required.

3.3 Requirements for Home/Remote Wireless Access

Connecting to the organization's network from a home or remote location via wireless must be done securely:

*   **Direct Network Access:** Wireless infrastructure devices (home routers) providing *direct* authenticated access to the organization's corporate network (e.g., via a hardware VPN tunnel directly terminating on the home router) must themselves be secured according to standards defined by the designated IT authority. This typically includes using WPA2/WPA3 Personal (PSK) with a strong passphrase, changing default admin credentials, disabling insecure features (like WPS

PIN), and keeping firmware updated. *(Refer to a detailed "Home Wireless Standard" or similar document if available, or detail specific requirements here).*
*   **Standard Remote Access:** If a home wireless network does not meet the standards for direct corporate access, connections to the organizational network must only occur via the standard, organization-approved remote access solution (e.g., software VPN client running on the endpoint device). The security of the home Wi-Fi (using at least WPA2-PSK with a strong password) remains the user's responsibility but does not directly impact the corporate network in this scenario due to the VPN tunnel originating from the endpoint.

3.4 Unauthorized Devices

Connecting unauthorized wireless access points or routers to the organization's wired network is strictly prohibited. Personal devices acting as Wi-Fi hotspots must not be connected to the corporate wired network.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including but not limited to, wireless network scanning, rogue AP detection systems, configuration audits of managed devices, security assessments, review of network logs, and investigation of reported incidents.

4.2 Exceptions

Any exception to the standards specified in this policy requires formal, documented justification, risk assessment, and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Non-compliant wireless devices may be disconnected from the network without notice. Violations of this policy by personnel may result in disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Definitions

*   **MAC Address (Media Access Control Address):** A unique identifier assigned to network interface controllers for communications at the data link layer. (While relevant to some wireless controls like MAC filtering, it's not a primary security mechanism required by this policy template).
*   **SSID (Service Set Identifier):** A name that identifies a specific wireless network.
*   **WPA2/WPA3 (Wi-Fi Protected Access versions 2 & 3):** Security protocols used to secure wireless networks. Enterprise modes use individual credentials via RADIUS; Personal modes use a Pre-Shared Key (PSK).
*   **EAP (Extensible Authentication Protocol):** An authentication framework used in WPA/WPA2/WPA3 Enterprise networks (e.g., EAP-TLS, PEAP).

*   **AES (Advanced Encryption Standard):** A strong encryption algorithm used within WPA2/WPA3.
*   **Rogue Access Point:** An unauthorized wireless access point connected to a network.

6.0 Related Policies

*   Acceptable Use Policy (AUP)
*   Password Policy
*   Remote Access Policy
*   Data Classification Policy
*   Lab Security Policy (if applicable)
*   Information Security Policy (Overall)
*   Baseline Workstation Configuration Standard (for client-side settings)

Revision #2
Created 28 August 2024 16:59:43 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery