[Insert Company Name and Logo]	
Title: Wireless Network Security	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy governs use of the organization's wireless networks and limits access to operational networks to authorized users.

Scope: This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the organization's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to [Insert Company name] networks do not fall under the purview of this policy.

Procedure:

1. [Insert Company name] wireless infrastructure must follow these guidelines:
    a. Design
        i. Configure a firewall between the wireless network and the wired infrastructure.
        ii. Ensure that 256-bit or higher encryption is used for all wireless communication.
        iii. Fully test and deploy software patches and updates on a regular basis.
        iv. Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.
        v. The guest network shall not connect to the [Insert Company name] network.
    b. Access Points (AP)
        i. Maintain and update an inventory of all Access Points (AP) and wireless devices.
        ii. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
        iii. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
        iv. The default settings on APs, such as those for SSIDs, must be changed.
        v. APs must be restored to the latest security settings when the reset functions are used.
        vi. Ensure that all APs have strong administrative passwords.
        vii. Enable user authentication mechanisms for the management interfaces of the AP.
        viii. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

ix. Turn on audit capabilities on AP; review log files on a regular basis.
x. Only wireless APs expressly authorized by the Security Officer shall be permitted to establish a connection.

c. Mobile Systems
   i. Install anti-virus software on all wireless clients.
   ii. Install personal firewall software on all wireless clients.
   iii. Disable file sharing between wireless clients.
   iv. All wireless devices shall be identified and authenticated prior to establishing a connection.

Violations:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Violation may also result in civil and criminal penalties to [Insert Company name] as determined by federal and state laws and regulations related to loss of data.

Attachments: None

Related Policies: Use of Mobile Devices

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.