# Securing Wireless Networks

This playbook outlines the steps necessary to secure a wireless network. It includes measures to protect against eavesdropping and unauthorized access, ensuring a safe and private wireless communication environment.

### Step 1: Change Defaults

Modify the default admin username and password of the wireless router to prevent unauthorized access.

### Step 2: Enable Encryption

Enable the highest level of encryption available (e.g., WPA3) on the wireless network to protect the data being transmitted over the air.

### Step 3: SSID Management

Change the Service Set Identifier (SSID) to a unique name that does not reveal the brand or model of the router, and disable SSID broadcasting to make the network less visible.

### Step 4: Filter MAC Addresses

Implement a MAC address filtering system to allow only recognized devices to connect to the wireless network.

### Step 5: Update Firmware

Regularly check and update the router's firmware to patch known vulnerabilities and improve security features.

### Step 6: Disable WPS

Turn off Wi-Fi Protected Setup (WPS) as it can be a security vulnerability due to certain flaws in its design.

### Step 7: Disable Remote Access

Disable remote access to the router's settings to ensure that configuration changes can only be made from a connection to the network itself, not from the internet at large.

### Step 8: Regular Audits

Conduct regular security audits to check for any unauthorized devices on the network and to ensure security features remain properly configured.

## General Notes

### Network Security

Securing a wireless network requires ongoing vigilance as new vulnerabilities can emerge. Regular updates and revisiting these security practices is recommended.

### Backup Settings

Before making changes to the router settings, ensure you backup the current configuration to expedite recovery in case of any misconfiguration.