# Documentation of Wireless Network Security Implementation

## Introduction

Wireless network security is critical to protecting sensitive data and ensuring uninterrupted operations. This document outlines the implementation of a secure wireless network using WPA3 encryption and a Wireless Intrusion Prevention System (WIPS) to prevent unauthorized access.

---

## 1. Wireless Network Security Configuration: WPA3

WPA3 (Wi-Fi Protected Access 3) is the latest standard for securing wireless networks, offering robust protection against attacks like brute force and improved encryption mechanisms.

**Configuration Details**

- **Network Name (SSID)**: SecureOffice_WiFi
- **Authentication Protocol**: WPA3-Personal (SAE - Simultaneous Authentication of Equals)
- **Encryption Standard**: AES-256
- **Additional Security Features**:
    - **Protected Management Frames (PMF)**: Enabled for enhanced communication protection.
    - **SSID Broadcasting**: Disabled to reduce network visibility.

**Steps to Configure WPA3:**

1. **Access Router Settings**:
    - Log in to the router's admin interface using a secure connection (e.g., `https://192.168.1.1`).
2. **Set Authentication Protocol**:
    - Navigate to the wireless settings and select WPA3-Personal as the authentication protocol.
3. **Enable PMF**:
    - In advanced security settings, activate PMF to secure management traffic.
4. **Set a Strong Passphrase**:
    - Use a passphrase of at least 16 characters, mixing uppercase, lowercase, numbers, and special characters.
5. **Save and Restart**:
    - Apply the changes and restart the router to implement the new security settings.

---

## 2. Wireless Intrusion Prevention System (WIPS)

WIPS is designed to monitor and prevent unauthorized access to the wireless network. It detects and mitigates threats such as rogue access points, deauthentication attacks, and unauthorized devices.

**Implementation Details**

- **WIPS Tool**: Cisco Wireless LAN Controller (WLC) with integrated WIPS capabilities.
- **Monitoring Frequency**: Continuous, covering 2.4 GHz and 5 GHz bands.
- **Detection Features**:
    - Rogue access point detection.
    - Detection of unauthorized clients attempting to connect.
    - Mitigation of MAC spoofing attacks.
- **Automated Response**:
    - Block rogue devices automatically.
    - Generate alerts for suspicious activities.

**Steps to Configure WIPS:**

1. **Activate WIPS**:
    - Access the WLC dashboard and enable the WIPS feature in the security settings.
2. **Define Threat Levels**:
    - Configure policies to categorize threats (e.g., rogue APs, unencrypted connections).
3. **Enable Auto-Mitigation**:
    - Set WIPS to automatically block devices violating security policies.
4. **Test the System**:
    - Simulate a rogue access point and confirm that WIPS detects and mitigates the threat.

---

## Conclusion

Implementing WPA3 encryption and WIPS ensures a robust security posture for wireless networks. WPA3 provides state-of-the-art encryption and protection against common wireless threats, while WIPS actively monitors and prevents unauthorized access. These measures significantly reduce the risk of data breaches and unauthorized network usage.