Wireless LAN Security Configuration Sample

1. Overview

This sample document provides a basic wireless LAN security configuration template for use in small to medium business environments.

2. Configuration Details

Setting	Value	Notes
SSID	Company-WiFi	Unique network name
Security Type	WPA2-Enterprise / WPA3	Use WPA3 if supported
Encryption	AES	Do not use TKIP
Authentication	802.1X with RADIUS	Certificate-based recommended
SSID Broadcast	Enabled	Do not hide SSID
MAC Filtering	Disabled	Not reliable as sole control
Guest Network	Enabled (Isolated)	VLAN separated

3. Sample Configuration (CLI)

```
interface Dot11Radio0
 ssid Company-WiFi
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii 0 [YourSecurePassphrase]
   encryption mode ciphers aes-ccm
!
interface Dot11Radio0
 no shutdown
!
interface FastEthernet0
 switchport mode access
!
```

Replace [YourSecurePassphrase] with a strong unique passphrase.

4. Access Point Setup Form

SSID

Company-WiFi

Security Type

WPA2-Enterprise

Encryption

AES

Authentication Method

802.1X (RADIUS)

Passphrase

Enter strong password

5. Best Practices

- Change default administration credentials on all access points.
- Disable WPS (Wi-Fi Protected Setup).
- Update firmware regularly.
- Segment guest traffic using VLANs.
- Monitor wireless usage and logs for unusual activity.
- Use strong unique passwords and rotate them periodically.