Secure Wireless Network Design Document

Project: [Project Name]
Date: [Date]
Prepared by: [Author Name]

1. Introduction

This document outlines the design and security considerations for the wireless network implementation at [Organization Name].

2. Objectives

- Provide secure and reliable wireless connectivity
- Ensure compliance with organizational policies and standards
- Support for guests and enterprise users
- Mitigate wireless threats and vulnerabilities

3. Network Topology

Overview of the planned wireless network architecture, coverage areas, and hardware locations.

Component	Type	Location
Access Point	[Model]	[Location]
Wireless Controller	[Model]	[Data Center]

4. Security Design

1. **Authentication:** WPA2/WPA3-Enterprise with RADIUS
2. **Encryption:** AES-CCMP
3. **Network Segmentation:** Separate VLANs for staff, guests, and IoT devices
4. **Firewall Rules:** Permit only necessary traffic between VLANs
5. **Monitoring:** Wireless Intrusion Detection & Logging

5. Access Control

- User authentication integrated with directory services (e.g., Active Directory)
- MAC address filtering for internal devices
- Guest access through self-service portal with temporary credentials

6. Management & Monitoring

- Centralized wireless management console
- Automated alerts for suspicious activities
- Regular security audits and vulnerability scans

7. Implementation Plan

1. Procure approved wireless equipment
2. Configure devices according to security requirements
3. Test coverage and performance in all intended areas
4. Conduct user acceptance testing
5. Go-live and handover to IT support team

8. References

- [Relevant Policy 1]
- [IEEE 802.11 Standards]
- [Manufacturer Documentation]

Document Revision History

Date	Version	Description	Author
[Date]	1.0	Initial Draft	[Author]