

Wireless Network Security Settings Policy

Document Title: Wireless Network Security Settings Policy

Version: 1.0

Prepared by: Muneer Shaukath

Next Review Date:

1. Purpose

To define minimum security requirements for the design, implementation, and management of the organization's wireless networks, ensuring the confidentiality, integrity, and availability of network services and data.

2. Scope

This policy applies to:

- All wireless access points (APs) owned and operated by the organization.
- All employees, contractors, and third-party users connecting to the organization's wireless networks.
- All devices connecting to the wireless network.

3. Policy Requirements

3.1 Wireless Network Segmentation

- Production LAN networks must be logically separated from guest networks and IoT devices.
- Guest wireless access must be isolated from the internal network.

3.2 Strong Encryption

- All wireless networks must use strong encryption protocols (WPA2-AES).
- WEP must not be used under any circumstances.

3.3 Strong Authentication

- Authentication must use strong credentials and/or enterprise-grade solutions (e.g., 802.1X with RADIUS).
- Default SSIDs, passwords, and admin credentials must be changed before deployment.

3.4 Access Point Configuration

- APs must have management interfaces secured and disabled from external access.
- Signal strength should be adjusted to limit coverage to the intended physical area.

3.5 Monitoring and Logging

- Wireless networks must be monitored for unauthorized access points (rogue AP detection).
- Logs of wireless network connections must be retained according to the log retention policy.

3.6 Guest and BYOD Controls

- Guests must connect to a separate VLAN with internet-only access.
- BYOD connections must comply with endpoint security requirements.

4. Non-Compliance

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, and possible legal action.

5. Review and Maintenance

This policy must be reviewed annually or whenever significant network infrastructure changes occur.

For Office Use Only:

Approved By: Sherry George	
Designation: Technical Director	
Signature:	
Reviewed by: Rixon Thomas	Date:

--End of Document--