Wireless Network Security Policy Sample

Policy Number: WNSP-001

Effective Date: [Insert Date]

Approved by: [Authority Name]

1. Purpose

This policy establishes the requirements for secure deployment and usage of wireless networks within [Organization Name] to protect sensitive information and assets from unauthorized access or disclosure.

2. Scope

This policy applies to all employees, contractors, consultants, and third-party workers who use, manage, or provide support for wireless networks within [Organization Name] facilities.

3. Definitions

Term	Definition
Wireless Network (Wi-Fi)	A network that allows devices to connect using radio signals.
SSID	Service Set Identifier; the public name of a wireless network.
WPA2/WPA3	Wi-Fi Protected Access version 2 or 3; encryption protocols for wireless security.

4. Policy

- All wireless access points must be authorized, documented, and approved by IT.
- Default SSIDs and passwords must be changed upon deployment.
- Enterprise-level encryption (WPA2 or WPA3) must be used on all wireless networks.
- Guest wireless access must be logically separated from internal resources.
- All wireless networks must require authentication for access.
- Periodic security assessments of wireless networks must be conducted.
- Users must not deploy rogue (unauthorized) wireless access points.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Review

This policy shall be reviewed annually and updated as needed to ensure compliance with evolving security standards.

7. Contact

For questions regarding this policy, contact the IT Department at [contact information].