Wireless Communication Policy

Last Update Status: *Updated October 2022*

1. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

2. Purpose

The purpose of this policy is to secure and protect the information assets owned by <Company Name>. <Company Name> provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. <Company Name> grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to <Company Name> network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a <Company Name> network.

3. Scope

All employees, contractors, consultants, temporary and other workers at <Company Name>, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of <Company Name> must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a <Company Name> network or reside on a <Company Name> site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4. Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a <Company Name> site and connect to a <Company Name> network, or provide access to information classified as <Company Name> Confidential, or above must:

4.1.1 Abide by the standards specified in the *Wireless Communication Standard*.
4.1.2 Be installed, supported, and maintained by an approved support team.
4.1.3 Use <Company Name> approved authentication protocols and infrastructure.
4.1.4 Use <Company Name> approved encryption protocols.
4.1.5 Maintain a hardware address (MAC address) that can be registered and tracked.
4.1.6 Not interfere with wireless access deployments maintained by other support organizations.

4.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to <Company Name> Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the <Company Name> network must:

4.2.1 Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the *Lab Security Policy*.
4.2.2 Not interfere with wireless access deployments maintained by other support organizations.

4.3 Home Wireless Device Requirements

4.3.1 Wireless infrastructure devices that provide direct access to the <Company Name> corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.
4.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the <Company Name> corporate network. Access to the <Company Name> corporate network through this device must use standard remote access authentication.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- MAC Address

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
October 2022	SANS Policy Team	Converted to new format.