Wireless Communication Policy

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 noesya. noesya provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. noesya 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 noesya network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Security Team are approved for connectivity to a noesya network.

3. Scope

All employees, contractors, consultants, temporary and other workers at noesya, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of noesya must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a noesya network or reside on a noesya 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

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

- Be installed, supported, and maintained by the Security Team.
- Use noesya approved authentication protocols and infrastructure.
- Use noesya approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

5. Policy Compliance

5.1. Compliance Measurement

The security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, internal audits, and feedback to the policy owner.

5.2. Non-Compliance

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

6. Revision History

1.0 Date of change: 01/09/2021 - Responsible: Technical team - Summary of Change: Initial release