Wireless Communication Policy

1 Overview

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.

2 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 personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

The Information Security Department must approve exceptions to this policy in advance.

3 Policy Statement

3.1 General Network Access 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, <Company Name> Highly Confidential, or <Company Name> Restricted must:

3.1.1   Abide by the standards specified in the Wireless Communication Standard.

3.1.2   Be installed, supported, and maintained by a approved support team.

3.1.3   Use <Company Name> approved authentication protocols and infrastructure.

3.1.4   Use <Company Name> approved encryption protocols.

3.1.5   Maintain a hardware address (MAC address) that can be registered and tracked.

3.1.6   Not interfere with wireless access deployments maintained by other support organizations.

3.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to <Company Name> Confidential, <Company Name> Highly Confidential, or <Company Name> Restricted information must adhere to section 3.1. Lab and isolated wireless devices that do not provide general network connectivity to the <Company Name> network must:

3.2.1   Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the DMZ Lab Security Policy or the Internal Lab Security Policy.

3.2.2   Not interfere with wireless access deployments maintained by other support organizations.

3.3 Home Wireless Device Requirements

3.3.1   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.

3.3.2   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.

4 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with <Company Name>.

5 Definitions

Term	Definition
<Company Name> network	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.
Corporate connectivity	A connection that provides access to a <Company Name> network.
Enterprise Class Teleworker (ECT)	An end-to-end hardware VPN solution for teleworker access to the <Company Name> network.
Information assets	Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
MAC address	The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

6 Revision History

Date of Change	Responsible	Summary of Change