Wireless Communication Policy

Defines the requirement for wireless infrastructure devices to adhere to wireless communication policy in order to connect to the company network.

Last Update Status: 19 *Dec, 2016*

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 BuildWealth Technologies Pvt Ltd. BuildWealth Technologies Pvt Ltd provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. BuildWealth Technologies Pvt Ltd 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 BuildWealth Technologies Pvt Ltd 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 BuildWealth Technologies Pvt Ltd network.

3. Scope

All employees, contractors, consultants, temporary and other workers at BuildWealth Technologies Pvt Ltd, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of BuildWealth Technologies Pvt Ltd must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a BuildWealth Technologies Pvt Ltd network or reside on a BuildWealth Technologies Pvt Ltd 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 BuildWealth Technologies Pvt Ltd site and connect to a BuildWealth Technologies Pvt Ltd network, or provide access to information classified as BuildWealth Technologies Pvt Ltd Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use BuildWealth Technologies Pvt Ltd approved authentication protocols and infrastructure.
- Use BuildWealth Technologies Pvt Ltd 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.

4.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to BuildWealth Technologies Pvt Ltd Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the BuildWealth Technologies Pvt Ltd network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.
- 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 BuildWealth Technologies Pvt Ltd 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 BuildWealth Technologies Pvt Ltd corporate network. Access to the BuildWealth Technologies Pvt Ltd 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, periodic walk through, video monitoring, 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.