Wireless Communication Standard

1. Overview

See Purpose.

2. Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Diocese network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Technical Services Team are approved for connectivity to a Diocese network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by a Technical Services approved support organization. Lab network devices must comply with the *Lab Security Policy*.

3. Scope

All employees, contractors, consultants, temporary and other workers at Diocese and its subsidiaries, including all personnel that maintains a wireless infrastructure device on behalf of the Diocese, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

The Technical Services Team must approve exceptions to this standard in advance.

4. Standard

4.1 General Requirements

All wireless infrastructure devices that connect to a Diocese network or provide access to Diocese Confidential, Diocese Highly Confidential, or Diocese Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

4.2 Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from Diocese production device SSID.
- Broadcast of lab device SSID must be disabled.

4.3 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a Diocese network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

5. Policy Compliance

5.1 Compliance Measurement

The Technical Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru's, 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 Technical Service 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