**Wireless Infrastructure Standard**

The **[Organization]** provides wireless connectivity options for employees, contractors, vendors, and agents in order to create a secure computing environment. In addition, guests are given the option of connecting to the Guest wireless network, which is a less secure environment for personal devices and gives limited access to resources.

# PurposeThe purpose of this standard is to provide guidelines which specify the technical requirements that wireless infrastructure devices must satisfy in order to connect to a [Organization] network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception as outlined in this standard are approved for connectivity to a [Organization] 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 [Department] or an [Department] approved support organization.

# Scope

# This standard applies to wireless devices that make a connection to the [Organization] network and all wireless infrastructure devices that provide wireless connectivity to the network.

# Standard

General Requirements
All wireless infrastructure devices that connect to a **[Organization]** network or provide access to **[Organization]** Protected 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 (SSP) with encryption enabled.

Lab or Wireless Device Requirements

* In the event a lab or test wireless infrastructure device needs to be set, the Service Set Identifier (SSID) must be different from any existing **[Organization]** production device SSID.
* Broadcast of these devices’ SSID must be disabled.

# Enforcement

This procedure is for your protection. Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

The Network Services and/or Cybersecurity teams will verify compliance with these procedures through various methods, including but not limited to: periodic walk-throughs, business tool reports, internal and external audits, and feedback to the procedure owner.

# Exceptions

Limited exceptions to the procedure must be approved by the **[management].**

1. **Definitions**
* Advanced Encryption Standard (AES): An encryption standard developed by the National Institute of Standards and Technology (NIST); intended to specify an unclassified, publically disclosed, symmetric Encryption algorithm.
* Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST): A lightweight connection protocol that replaced Lightweight Extensible Authentication Protocol (LEAP.)
* Extensible Authentication Protocol-Translation Layer Security (EAP-TLS): An open standard that uses the Transport Layer Security (TLS) protocol; the original, standard wireless LAN EAP authentication protocol.
* Protected Extensible Authentication Protocol (PEAP): A protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated TLS tunnel.
* Service Set Identified (SSID): A case sensitive unique identifier attached to the header of packets sent over a wireless local-area network (WLAN); the broadcast name of the network.
* Secure Simple Pairing (SSP): A feature of Bluetooth that was created to address concerns related to security and the simplicity of the pairing process.
* Temporal Key Integrity Protocol (TKIP): An encryption protocol included in the IEEE 802.11i standard for Wireless LANs; provides more secure encryption than the original WLAN security protocol (WEP.)