

Provo City School District Technology Security Policy

Wireless Infrastructure Communication Procedure

Last Update Status: *Updated January 2015*

1. Overview

Proper configuration and deployment of wireless infrastructure devices is essential to the PCSD network. Incorrectly configured wireless infrastructure devices can provide an attacker easy access to a network. Poorly deployed wireless infrastructure devices can disrupt/degrade wireless communication between devices.

2. Purpose

This procedure specifies the technical requirements that wireless infrastructure devices must satisfy to connect to the PCSD network. Only those wireless infrastructure devices that meet the requirements specified in this procedure or are granted an exception by the InfoSec team are approved for connectivity to the PCSD network.

Network devices including, but not limited to controllers, routers, switches, firewalls, remote access devices, or wireless access points, must be installed, supported, and maintained by PCSD Network Team.

3. Scope

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

The InfoSec Team must approve exceptions to this procedure in advance.

4. Procedure

PCSD Wireless Device Requirements

- All wireless infrastructure devices that connect to a PCSD network or provide access to Confidential, Highly Confidential, or 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 Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
 - Be configured and deployed by PCSD Networking.
 - All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

Provo City School District Technology Security Policy

- Lab and Isolated Wireless Device Requirements
 - Lab device Service Set Identifier (SSID) must be different from PCSD production device SSID.

Home Wireless Device Requirements

- All home wireless infrastructure devices that provide direct access to a PCSD network, via VPN, must adhere to the following:
 - Enable at the minimum WPA2
 - When enabling WPA2, configure a complex shared secret key (at least 10 characters) on the wireless client and the wireless access point
 - Change the default SSID name
 - Change the default login and password (Should follow the Password Procedures)