Provo City School District Technology Security Policy

Audit Procedure

Last Update Status: *Updated January 2015*

1. Overview

Planned and random security audits are important in order to mitigate risk and evaluate our preparedness for a security incident. The InfoSec Team will conduct periodic audits on devices connected to the PCSD network.

2. Purpose

The purpose of this procedure is to ensure all devices are configured according to the PCSD security policy. All devices connected to the PCSD network are subject to audit at any time. Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Ensure conformance to the PCSD security policy

3. Scope

This procedure covers all devices owned or operated by PCSD. This procedure also covers any device present on the PCSD network, including devices that may not be owned or operated by PCSD.

4. Procedure

PCSD hereby provides its consent to allow the InfoSec team or an external auditor to access its devices to the extent necessary, within a predetermined scope; which will be written and approved by the InfoSec team to allow the auditor to perform scheduled and random audits of any/all devices at PCSD.

- Specific Concerns
  PCSD devices may support critical business functions and store sensitive information. Improper configuration of devices could lead to the loss of confidentiality, availability or integrity of these systems

- Guidelines
  Approved and standard configuration templates shall be used when deploying devices:
  - Host security agents such as antivirus shall be installed and updated
  - Perform network scans to verify only required network ports and network shares are in use
  - Verify administrative group membership
  - Conduct baselines when systems are deployed and upon significant system changes
  - Changes to configuration template shall be coordinated with appropriate IT members
  - Must follow all other applicable procedures for deployed devices

Provo City School District Technology Security Policy

- Responsibility
  The InfoSec Team or an external auditor shall conduct audits of all devices owned or operated by PCSD. Device owners are encouraged to audit their own devices as needed; this does not allow a device owner to perform an audit of the PCSD network or on any device not owned by the employee

- Relevant Findings
  All relevant findings discovered as a result of an audit shall be listed in the PCSD tracking system to ensure prompt resolution and/or appropriate mitigating controls

- Ownership of Audit Report
  All results and findings generated by the InfoSec team or an external auditor must be provided to appropriate PCSD management within one week of project completion. This report will become the property of PCSD and be considered confidential