Provo City School District Technology Security Policy

Server Security Procedure

Last Update Status: *Updated January 2015*

1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2. Purpose

The purpose of this procedure is to establish standards for the base configuration of internal server equipment that is owned and/or operated by PCSD. Effective implementation of this procedure will minimize unauthorized access to PCSD proprietary information and technology.

3. Scope

All employees, contractors, and consultants must adhere to this procedure. This procedure applies to server equipment that is owned, operated, or registered under the PCSD internal network domain.
This procedure specifies requirements for equipment on the internal network.

4. Procedure

General Requirements

- All internal servers deployed at PCSD must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the InfoSec Team. Operational groups should monitor configuration compliance and implement an exception procedure tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the InfoSec Team. The following items must be met:
- Servers must be registered with the inventory management system and a CSI (Critical System Information) document must be created. At a minimum, the following information is required:
    - Server contact(s) and location, and a backup contact and location
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
    - Serial number
    - HW address
    - Purchase information
    - Support information
    - Vendor information
        - Information in the inventory management system and CSI must be kept up-to-date.

- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Procedure*.
- Configuration Requirements
- Operating System configuration should be in accordance with approved InfoSec guidelines
- Services and applications that will not be used must be disabled where practical
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with teaching and instruction
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient
- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec)
- Servers should be physically located in an access-controlled environment
- Servers are specifically prohibited from operating from unauthorized devices and networks
- Monitoring
- All security-related events on critical or sensitive systems must be logged
- Security-related events will be reported to the InfoSec Team, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host