

# Provo City School District Technology Security Policy

## Employee Security Awareness Training Procedure

**Last Update Status:** *Updated January 2015*

### 1. Overview

The most effective way to make sure that PCSD employees will not make costly errors in regard to information security is to institute district-wide security-awareness training initiatives that include, but are not limited to: instructor led training sessions, mandatory yearly SafeSchools customized training for all employees, additional required SafeSchool training requirements for employees that have access to sensitive information. Tools available are: a security awareness website, helpful hints via e-mail, tech talk publications, posters, and promotions.

### 2. Purpose

These methods help ensure employees have a solid understanding of our security policy, procedures, and best practices. Employees shall also have a basic understanding of the following security related topics: social engineering tactics, e-mail and messaging security, safely browsing the internet, social networking threats, mobile device security, password best practices, data classification, data transmission and encryption, data destruction, Wi-Fi security, working remotely, insider threats from students and staff, physical security issues, protecting personal/work computers, copyright infringements, malware and virus protection, sharing files with local and state entities, and workspace security.

### 3. Scope

All PCSD employees shall receive security-specific trainings annually.

### 4. Procedure

The following types of training will be implemented:

- Instructor led training as needed
- SafeSchools training videos and certificates
  - Basic security video training to be completed yearly by all employees.
  - Additional, more in-depth training required for users who have access to P.I.I.
  - Completion of the training to be monitored by Human Resources (HR).
- Security Awareness website
  - General information
  - Video resources
  - Links to our policies and procedures.
  - Links to additional information on the web.
- Helpful Hints
  - Notifications will be sent when there is a significant security risk or threat.
  - Continue to send out Tech Talk Newsletters regarding information security.

Utilize any other means necessary to inform our employees of security information or training opportunities.