Provo City School District Technology Security Policy

Remote Access Procedure

Last Update Status: *Updated January 2015*

1. Purpose

The purpose of this procedure is to define standards for connecting to PCSD's network from any host. These standards are designed to minimize the potential exposure to PCSD from damages, which may result from unauthorized use of PCSD resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical PCSD internal systems, etc.

2. Scope

This procedure applies to all PCSD employees, contractors, vendors and agents with a PCSD-owned or personally owned computer or workstation used to connect to the PCSD network. This procedure applies to remote access connections used to do work on behalf of PCSD, which includes reading or sending email, accessing PCSD servers, and viewing intranet web resources.

Remote access implementations that are covered by this procedure include, but are not limited to DSL, VPN, and SSH.

3. Procedure

It is the responsibility of PCSD employees, contractors, vendors and agents with remote access privileges to PCSD's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to PCSD.

Please review the following procedures to ensure protection of information when accessing the PCSD network via remote access methods, and acceptable use of PCSD's network:

- *Encryption Procedures*
- *Wireless Infrastructure Communications Procedure*
- *Acceptable Use Procedure*

Requirements

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the *Password Procedures*.
- At no time should any PCSD employee provide his or her login or email password to anyone, not even family members.
- PCSD employees with remote access privileges must ensure that their PCSD-owned or personal computer or workstation, which is remotely connected to PCSD's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- The InfoSec Team must approve non-standard hardware configurations. Security configurations for access to hardware must also be approved.

- All hosts that are connected to PCSD internal networks via remote access technologies, must use the most up-to-date anti-virus software, this includes personal computers.
- Personal equipment that is used to connect to PCSD's networks must meet the requirements of PCSD-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the PCSD production network must obtain prior approval from PCSD Tech Support.