Remote Access Procedure

Last Update Status: *Updated Mar 2018*

The purpose of this procedure is to define standards for connecting to Provo City School District's (PCSD) 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 district confidential data, intellectual property, damage to public image, damage to critical PCSD internal systems, etc. 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 VPN, and SSH.

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.

Requirements

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong passphrase see *Password Procedures*.
- At no time should any PCSD user provide his or her login or email password to anyone, not even family members.
- PCSD users 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.
- All hosts that are connected to PCSD internal networks via remote access technologies, must use up-to-date anti-virus software, this includes personal computers.
- 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.

Security Response Plan

Last Update Status: *Mar 2018*

General Information

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. Provo City School District (PCSD) operations rely on the proper use of Confidential Information and Personally Identifiable Information (PII) on a daily basis. Managing risk and responding in an organized way to incidents and breaches is key to operations.

This policy is designed to standardize the PCSD-wide response to any reported breach or incident and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

Standardized processes and procedures help to ensure the PCSD can act responsibly, respond effectively, and protect its information assets from unauthorized use to the extent possible. The purpose of this procedure is to ensure that the security Incident Response Team (IRT) has all the necessary information to formulate and execute a successful response should a specific security incident occur.

The development, implementation, and execution of a Security Response Plan (SRP) are primarily the responsibility of the specific operational group. Operational groups (OpGroups) are expected to properly facilitate the SRP applicable to the service or products for which they are accountable. Each OpGroup Coordinator is further expected to work with the Information Security Manager (InfoSec Manager) in the development and maintenance of the SRP.

Contact Information

Contact information for OpGroup Coordinator and InfoSec Manager must be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product. This document must include reference to current phone numbers and email address for the dedicated team member(s).

Data Classification

Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that PCSD management respond quickly and identify the data classification of the incident. This allows staff to respond accordingly in a timely and thorough manner.

Data classification shall refer to the following PCSD data categories:

Public Data - Information intended for public and community use or information that can be made public without any negative impact on the PCSD or its customers. Student PII shall never be considered public data unless the data has been defined as Directory Information.

Confidential/Internal Data - Information of a more sensitive nature to the business and educational operations of PCSD. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within PCSD. Employee and Educator PII (with the exception of social security numbers, financial information, or other critical information) falls within this classification.

Highly Confidential Data- Information that, if breached, causes significant damage to PCSD operations, reputation, and/or business continuity. Access to this information should be highly restricted. Student PII falls into this category of data. Employee or Educator Financial Information, Social Security Numbers, and other critical information also fall into this classification.

Data Breaches or Incidents Classification:

Critical/Major Breach or Incident – Incidents or breaches in this category deal with Confidential Information or PII and are on a large scale (PCSD-wide). All incidents or breaches involving Student PII will be classified as Critical or Major. They typically have the following attributes:

- Significant Confidential Information or PII loss, potential for lack of business continuity, PCSD exposure, or irreversible consequences are imminent

- Negative media coverage is likely and exposure is high
- Legal or contractual remedies may be required
- Any breach of contract that involves the misuse or unauthorized access to Student PII by a School Service Contract Provider

Moderately Critical/Serious Incident – Breaches or incidents in this category typically deal with Confidential Information and are on a medium scale (e.g. <100 users on the internal network, application or database related, limited exposure). Incidents in this category typically have the following attributes:

- Third party service provider and subcontractors may be involved
- Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized PCSD exposure
- Service outages are likely while the breach is addressed
- Negative media coverage is possible but exposure is limited
- Disclosure of Educator or Employee PII is contained and manageable

Low Criticality/Minor Incident – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale (e.g. <10 users on the internal network, personal or mobile device related). Incidents in this category typically have the following attributes:

- User inconvenience is likely but not PCSD damaging
- Internal data released but data is not student, employee, or confidential in nature
- Incident can be addressed through normal support channels

Incident Reporting

The following process shall be followed when responding to a suspected incident:

Confirmed or suspected incidents shall be reported promptly to the InfoSec Manager. If the InfoSec Manager is unavailable, notify the next person on the list until someone has been contacted. It is then the responsibility of the contacted team member to take action or contact the appropriate resource. A formal report shall be filed that includes full and accurate details of the Incident including who is reporting the Incident and what classification of data is involved.

Once an Incident is reported, the InfoSec Manager shall conduct an assessment to establish the severity of the incident, next steps in response, and potential remedies and solutions. Based on this assessment, the InfoSec Manager shall determine if this incident remains an incident or if it needs to be categorized as a breach.

All incidents and breaches will be centrally logged and documented to ensure appropriate documentation, oversight, and consistency in response, management, and reporting.

Assess, Contain and Recover Data

All security incidents shall have immediate analysis of the incident and an incident report completed by the InfoSec Manager or their designee. This analysis shall include

- A determination of whether this incident should be characterized as a breach including the

severity of the incident and the sensitivity of the data involved
- Identify the cause of the incident and whether the breach has been contained
- Determine the loss or potential loss of data, and limit exposure/damages. Were there any legal, contractual or regulatory requirements involved?
- Identify any users whose data may be compromised and notify them if needed
- Recover any data possible through backups or other available means
- Record of information found and steps taken during the investigation

The analysis of the information shall be documented and shared with the Incident Response Team, the affected parties, and any other relevant stakeholders.

Post Mortem Evaluation and Response

Each incident or breach determined to be "moderately critical" or "critical" shall have a post mortem analysis completed by the InfoSec Admin and the Incident Response Team to appropriately document, analyze, and make recommendations on ways to limit risk and exposure in the future.

Security for Sensitive Workstations Procedure

Last Update Status: *Updated Mar 2018*

The purpose of this procedure is to ensure the security of information that a sensitive workstation may have access to. Additionally, the procedure provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met. These workstations will be identified by the InfoSec team**.** Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and limited availability of sensitive information, including protected health information (PHI). Access to sensitive information will be restricted to authorized users.

- PCSD employees using controlled workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.
- PCSD will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to only authorized users.
- Appropriate measures include:
  - Restricting physical access to workstations to only authorized personnel.
  - Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
  - Enabling a password-protected screensaver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with PCSD *Password Procedure*.
  - Complying with all applicable password policies and procedures. See PCSD *Password Procedure*.
  - Ensuring controlled workstations are used for authorized business purposes only.
  - Never installing unauthorized software on controlled workstations.

- Storing all sensitive information, including protected health information (PHI) only on secured network servers
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the *Encryption Procedure*
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Exit running applications and close open documents.
- If wireless network access is used, ensure access is secure by following the *Wireless Device Communication procedure.*

Wireless Device Communication Procedure

Last Update Status: *Updated Mar 2018*

The purpose of this procedure is to secure and protect assets owned by PCSD. PCSD provides computer devices, networks, and other electronic information systems, to meet missions, goals, and initiatives. PCSD grants access to these resources as a privilege, and must manage them responsibly to maintain the confidentiality, integrity, and availability of all assets. This procedure specifies the conditions that wireless infrastructure devices must satisfy to connect to the PCSD network. Only those wireless devices that meet the standards specified in this procedure or are granted an exception by the InfoSec team are approved for connectivity to a PCSD network.

Devices must:

- Use PCSD approved authentication protocols, encryption protocols and infrastructure.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Be approved by the Technology Department.

Home Wireless Network 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 12 characters) on the wireless client and the wireless access point.
- Change the default wireless SSID name.
- Change the router default login and password. see *Password Procedures*