Audit Procedure

Last Update Status: *Updated September 2015*

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. 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, availability of information and resources, and to ensure conformance to the PCSD security policy.

PCSD hereby provides its consent to allow the InfoSec team or an approved 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. The InfoSec Team or third party (under contract) may 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**. 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.

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.

Clean Desk Procedure

Last Update Status: *Updated May 2017*

The purpose of this procedure is to establish a culture of security for all PCSD employees. An effective clean desk effort, involving the participation and support of all employees, will protect paper documents that contain personally identifiable and other sensitive information about students, educators and staff. A clean desk procedure reduces the threat of a security incident since confidential information will be locked away when unattended.

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including but not limited to Personally Identifiable Information (PII). Appropriate measures include:

- Restricting physical access to devices.
- Ensuring that all sensitive/confidential information in hardcopy or electronic form is secure in the work area at the end of each day.
- Securing workstations (screen lock or logout) prior to leaving an area to prevent unauthorized access.
- Enabling a password-protected screensaver with a short timeout period to ensure that devices left unsecured will be protected.
- Complying with all applicable password policies and procedures. See PCSD's *Password Procedure*.
- Ensuring devices are used for authorized educational/business purposes only.
- Never sending PII via email to anyone, including forwarding a message.

- Storing all sensitive information on password-protected drives or secure, restricted, network servers.
- Securing laptops that contain sensitive information by using cable locks, locking laptops up in drawers or cabinets, and/or by locking the door behind you.
- Sensitive working papers should be locked in a secure drawer whenever a user is away from their desk.
- At the end of the work-day the employee is expected to tidy their desk by locking up all sensitive papers and devices.

Email Procedure

Last Update Status: *Updated May 2017*

Email is commonly used throughout the district. Misuse of email, however, can pose many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications. The purpose of this email procedure is to ensure the proper use of the PCSD email system and make users aware of what PCSD deems as acceptable and unacceptable use of its email system.

- All use of email must be consistent with PCSD policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- PCSD email account should be used primarily for PCSD business-related purposes; personal communication is permitted on a limited basis, but non-PCSD related commercial uses are prohibited.
- The PCSD email system shall not to be used for the creation or distribution of any disruptive or offensive messages; including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any PCSD employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding PCSD email to a third-party email system. Individual messages which are forwarded by the user must not contain PCSD confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as ~~Google,~~ Yahoo, and MSN Hotmail etc. to conduct PCSD business, to create or memorialize any binding transactions, or to store or retain email on behalf of PCSD. Such communications and transactions should be conducted through proper channels using PCSD-approved documentation.
- Using a limited amount of PCSD resources for personal emails is acceptable. Sending chain letters or inappropriate joke emails from a PCSD email account is prohibited.
- PCSD employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- PCSD may monitor messages without prior notice. PCSD is not obligated to monitor email messages.

Employee Security Awareness Training Procedure
(Grayed items contained in Data Governance Policy)

Last Update Status: *Updated May 2017*

Security Awareness Procedure

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 SafeSchools training requirements for employees that have access to sensitive information. Tools available include a security awareness website, helpful hints via e-mail, tech talk publications, posters, and promotions. 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. All PCSD employees shall receive security-specific trainings annually.

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
- 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

General Password Procedure

Last Update Status: *Updated May 2017*

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the entire network. The purpose of this procedure is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

To minimize the possibility of unauthorized access, all passwords should meet or exceed the guidelines for creating strong passwords.

Password Characteristics:

Strong passwords

- Contain at least 8 alphanumeric characters
- Contain both upper and lower case letters
- Contain at least one number (for example, 0-9)
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

Poor or weak passwords

- Contain less than twelve characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon
- Contain personal information such as birth dates, addresses, phone numbers, names of family members, pets, friends, ~~and~~ fantasy characters, and other information found easily on social media or the internet.
- Contain work-related information such as building names, mascots, hardware, or software
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

Password Procedure (*Bolded procedures apply to Administrators*)

- Users must not use the same password for PCSD accounts as for other non-PCSD access (for example, personal email accounts, shopping sites, social media, and so on).
- Where possible, users must not use the same password for various PCSD access needs.
- **User accounts that have system-level privileges granted through group memberships or programs such as PowerSchool must have a unique password from all other accounts held by that user to access system-level privileges; accounts must have 2-factor authentication enabled when possible.**
- You should never write down or store passwords without acceptable encryption. Instead, try to create passwords that can be remembered easily without using common information known about you.
- **All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a yearly basis.**
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least annually. The recommended change interval is every four months
- Password cracking or guessing may be performed on a periodic or random basis by the InfoSec team or its delegates. If a password is guessed or cracked during one of these scans, the user will be notified and required to change it immediately.
- Systems that can force password change must force regular password changes.
- Default passwords must be changed during initial setup and configuration.
- The Technology help desk manages forgotten passwords and password resets. Be prepared to answer some questions to verify your identity.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted along with the username into email messages or other forms of electronic communication.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share your PCSD passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a

file on a computer system or mobile devices (phone, tablet) *without* encryption.
- Never use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident to their supervisor and change all passwords immediately.
- Use Auto-logout on systems that allow it.

Software Installation Procedure

Last Update Status: *Updated May 2017*

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions, older versions of software, or pirated software can prevent programs from running. These and other issues can introduce malware from infected installation software and expose unlicensed software that would be discovered during an audit. Programs, which can be used to compromise the organization's network, are also examples of the problems that can be introduced when employees install software on company equipment. The purpose of this procedure is to outline the requirements around installation software on PCSD computing devices. It's purpose is to minimize the risk of loss of program functionality, the exposure of sensitive information contained within PCSD's network, the risk of introducing malware, and the legal exposure of running unlicensed software.

Procedure

- Employees that handle sensitive information may not install any software that is not District approved. All other Employees may install personal purchased software on PCSD's computing devices operated within the district network with the understanding that it will not be supported by the Help Desk staff in any way. You must contact the manufacturer for assistance. Be sure to check the system requirements on the packaging prior to purchase and installation.
- Copies of "borrowed" software are prohibited. One (1) license equals one (1) installation.
- District Supported Software must be selected from an approved software list, maintained by the Information Technology department. If a specific program is not listed, you may request the purchase through your school's purchasing protocols, keeping in mind that there will be no district support.
- The assigned Information Technology Department representative (purchaser) will obtain and track the licenses of district-supported software only, test new software for conflict and compatibility, and perform the installation.
- The user should not uninstall District software, upon termination all District owned software shall be removed from the device.
- All employees who choose to connect a personal device on the district network must abide by the same procedure as pertained to district owned devices. The OS software is the responsibility of each user. All computers must have antivirus software installed prior to connection to the district network. If antivirus software is removed the user will lose access to the District network.
    - No district licensed software can or will be installed on a personal device. If an individual requires the Microsoft Office Suite, for example, they will need to purchase that through third party retailers or opt to use free suites such as OpenOffice or LibreOffice.
    - District tech support will only be provided to insure that the user is able to connect to the network.