Technology Security Plan

Introduction

Purpose

The purpose of this plan is to ensure the secure use and handling of all Park City School District (PCSD) data, computer systems and computer equipment by PCSD students, patrons, and employees.

It is the policy of PCSD to support secure network systems in the district, including security for all personally identifiable information that is stored digitally on PCSD-maintained computers, networks and storage devices. This policy supports efforts to mitigate threats that may cause harm to PCSD, its students, or its employees.

PCSD will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

All persons who are granted access to the PCSD network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of PCSD devices and the network. When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the PCSD's Information Security Manager with the relevant information.

This policy and procedure also covers third party vendors/contractors that contain or have access to PCSD critically sensitive data. All third party entities will be required to abide by all federal and state privacy and data governance laws and by all PCSD policy before accessing our systems or receiving information.

It is the policy of PCSD to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this plan are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Office of Education. PCSD supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect PCSD's data, users, and electronic assets.

Non-Compliance

Non-compliance with the requirements of this plan may result in loss of access to PCSD Data or PCSD network on which it is maintained. Employees and contractors may be subject to disciplinary action, up to and including termination of employment, and termination of any agreement under which contract work is performed.

Definitions

Access: Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.

Computer network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

Computer property: Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

Encryption or encrypted data: The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Personally Identifiable Information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered Protected data

System Security: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

Sensitive data: Data that contains personally identifiable information.

Administrative Access: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

Firewall: a network security device that monitors traffic to or from your computer network. It allows or blocks traffic based on a defined set of security rules.

Operating System: the software that supports a computer's basic functions, such as scheduling tasks, running applications, printing and controlling external devices.

Software Patch or Software Update: a piece of software designed to update a computer program or its supporting data to fix or improve its function. This includes fixing security vulnerabilities and/or other bugs.

Virus Protection Software: a program that analyzes programs or data to see if the program or data are trying to obtain information or to steal data for the purpose of using it maliciously. It is used to prevent viruses, worms, trojan horses, etc from getting onto a computer as well as remove any malicious software code known to infect a computer.

Security Responsibility

PCSD shall appoint, in writing, an IT Security Manager (ISM) responsible for overseeing district-wide IT security, to include development of PCSD policies and adherence to the standards defined in this document.

The IT Security Manager for PCSD will be Joe Stout, Director of Technical Support.

Training

PCSD shall ensure that all PCSD employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all PCSD employees.

PCSD shall ensure that all students are informed of Cyber Security Awareness.

Access Security

Computer Security

PCSD shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. A screen lock to computer systems is set between 1 to 15 minutes on all PCSD faculty and student computers. This ensures users must enter their password before access to system is allowed.

PCSD shall ensure that all equipment that contains sensitive information will be secured to deter theft.

Server/Network Room Security

PCSD shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or district office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or other designated staff members having access necessary to perform their job functions. No other staff or visitors are allowed unescorted access.

Telecommunication rooms/closets may only remain unlocked or unsecured when a building design makes it impossible to secure otherwise or due to environmental problems that require the door to be opened.

Contractor access

Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access will need to be confirmed and escorted directly by an authorized PCSD IT Employee.

Network Security

Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

Network Segmentation

PCSD shall ensure that all untrusted and public access computer networks are separated from main PCSD computer networks and utilize security policies to ensure the integrity of those computer networks.

PCSD will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

Wireless Networks

No wireless access point shall be installed on PCSD's computer network that does not conform with current PCSD network standards as defined by the Network Administrator. Any exceptions to this must be approved directly in writing by the ISM.

PCSD shall scan for and remove or disable any rogue wireless devices on a regular basis.

All wireless access networks shall conform to current PCSD best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

Remote Access

PCSD shall ensure that any remote access with connectivity to PCSD's internal network is achieved using PCSD's centralized VPN service that is protected by multiple factor authentication systems.

Access Control

System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

Authentication

PCSD shall enforce strong password management for employees, students, and contractors. All server system-level passwords must conform to the current PCSD password guidelines.

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords immediately.

Authorization

PCSD shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

PCSD shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

Accounting

PCSD shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.

Administrative Access Controls

PCSD shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

Incident Management

Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

PCSD shall develop and deploy a pan in the event of a known data breach to determine a proper course of action for notifying the proper person(s) and/or people who are affected by the data breach.

Business Continuity

To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of PCSD IT operations.

PCSD shall develop and deploy a district-wide business continuity plan which should include as a minimum:

- **Backup Data:** Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
- **Secondary Locations:** Identify a backup processing location, such as another School or District building.
- **Emergency Procedures:** Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.

Malicious Software

Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

PCSD shall install, distribute, and maintain spyware and virus protection software on all PCSD-owned equipment, i.e. servers, workstations, and laptops.

PCSD shall ensure that malicious software protection will include frequent update downloads, frequent scanning, and that malicious software protection is in active state (real time) on all operating servers/workstations.

PCSD shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.

All computers that will be connected to the PCSD wired or wireless secure network must use the PCSD approved anti-virus software or solution.

Any exceptions to this section must be approved by the ISM.

Internet Content Filtering

In accordance with Federal and State Law, PCSD shall filter internet traffic for content defined in law that is deemed harmful to minors.

PCSD acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, PCSD uses a combination of technological and supervisory means to protect students from harmful online content while in our schools.

In the event that students take devices home, PCSD will provide a technology based filtering solution for those devices. However, PCSD will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content while away from the schools.

Data Privacy

PCSD considers the protection of the data it collects on students, employees and their families to be of the utmost importance. PCSD protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (“FERPA”), the Government Records and Management Act U.C.A. §62G-2 (“GRAMA”), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 (“COPPA”), Utah Administrative Code R277-487 (“Student Data Protection Act”), and the PCSD Data Governance Plan.

PCSD shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

In the event of an investigation of employee or student data, the investigating authority must work with the ISM for the confiscation or access of any PCSD computer or server.

Security Audit and Remediation

PCSD shall perform routine security and privacy audits in congruence with the PCSD’s Information Security Audit Plan.

PCSD personnel shall develop remediation plans to address identified lapses that conforms with the PCSD Information Security Remediation Plan Template.

Related Documents

- Student Data Protection Act, Utah Code Ann. §§ 53A-1-1401 et seq.
- Utah Family Educational Rights and Privacy Act, Utah Code Ann. §§ 53A-13-301 et seq.
- District Acceptable Use Policy 9110
- District Family Educational Rights and Privacy Policy 11000
- District Records Management Policy 4020
- District Data Governance Plan
- District Student Data Disclosure Statement