



Cache County School District

Policy Series 6000: Finance and Operations

Policy No. 6900 P2

Information Technology Security Procedure

Plan

The Information Technology Security procedures, in alignment with Data Governance procedures, aim to ensure the secure use and handling of all district data, computer and networking systems, and other equipment by students, patrons, and employees. CCSD is committed to supporting secure network systems, processes, and procedures to protect all personally identifiable or confidential information stored, whether on paper or digitally, in district facilities or on district-maintained servers, computers, and networks. This procedure is designed to mitigate threats that could harm the district, its students, or its employees.

Definitions

- A. Access: To 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.
- B. 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 personally identifiable information.
- C. Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.
- D. Computer network: The interconnection of communication or telecommunication lines between: computers; computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.
- E. 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.
- F. 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.
- G. 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.
- H. Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password



Cache County School District

Policy Series 6000: Finance and Operations

protection, other forced authentication, or access control designed to keep out unauthorized persons.

- I. Sensitive data System level: Data that contains personally identifiable information.
- J. System level: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

Framework

- A. CCSD shall adopt a cyber security framework that offers guidance on security practices.
 - a. CIS Critical Security Controls shall be the framework that is adopted by the district and implemented by the Technology Department and Security Officer.
 - b. Best efforts will be made to follow the guidance of the security framework while acknowledging the complexities that arise in K-12 education networks.

Training

- A. All staff should complete IT security training annually which covers phishing, general cyber security, and other topics deemed necessary by the IT Security Officer to meet safety and cybersecurity requirements. New employees shall complete this training within 60 days of start date.
- B. Cyber security awareness should be included in digital citizenship content shared with students annually.

Physical Security

- A. Computer Security
 - a. Employees should not leave computers unattended and unlocked, particularly when accessing sensitive systems or data, such as student or employee information. To ensure compliance, automatic log-offs or system locks should be utilized.
 - i. Employees are responsible for manually logging out of student or employee information systems when not actively being used.
 - ii. Employees should log off or lock devices when leaving their vicinity if others might reasonably gain access.
- B. Server/Network Room Security
 - a. CCSD 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 methods, with only those IT or other staff members requiring access necessary to perform their job functions

Cache County School District

Policy Series 6000: Finance and Operations

allowed unescorted access.

- b. Cameras should cover the entrance of the server room and may be included inside server rooms and/or main data closets at each location as determined by the Security Officer or Director of Technology.
 - c. Telecommunication rooms/closets may only remain unlocked or unsecured when, because of building design, it is impossible to do otherwise, or due to environmental problems that require the door to be opened.
- C. Contractor Access
- a. 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 directly by the authorized employee who issued the service request or by CCSD's Technology Department.
 - b. Work in server rooms should only be done while a member of the Technology Department is present.

Network Security

- A. 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 shall require encryption where technologically feasible.
- B. Network Segmentation
- a. CCSD shall ensure that all untrusted and public access computer networks are separated from main district computer networks, and utilize security policies to ensure the integrity of those computer networks.
 - b. CCSD 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 to minimize potential damage from other compromised systems.
- C. Wireless Networks
- a. No wireless access point shall be installed on CCSD's computer network that does not conform with current network standards as defined by the Network Manager. Any exceptions to this must be approved directly in writing by the Security Officer.
 - b. CCSD shall scan for and remove or disable any rogue wireless devices on a regular basis.
 - c. All wireless access networks shall conform to current best practices and shall utilize, at minimal, WPA2 encryption for any connections. Open access networks



Cache County School District

Policy Series 6000: Finance and Operations

are not permitted, except on a temporary basis for events when deemed necessary by the Director of Technology, or when a district provided Wireless SSID utilizes open access to direct known users to more secure Wireless SSIDs.

D. Remote Access

- a. CCSD shall ensure that any remote access with connectivity to the district's internal network is achieved using the district's centralized VPN service or approved remote access system, which shall be protected by multiple factor authentication (MFA). Any exception to this plan must be due to a service provider's technical requirements and must be approved by the Security Officer.

Access Control

- A. 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.

B. Authentication

- a. CCSD shall enforce strong password management for employees, students, and contractors.
- b. Password Creation
 - i. Password length and complexity will be guided by the district's approved security framework.
 - ii. All server system-level passwords must conform to the Password Construction Guidelines posted by the Security Officer internally.
- c. Password Protection
 - i. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
 - ii. Passwords must not be inserted into email messages or other forms of electronic communication.
 - iii. Passwords must not be revealed over the phone to anyone. CCSD will never ask for a password from a user.
 1. Temporary passwords may be shared with end users by Help Desk or other Technology Department staff; which the end user shall change immediately.
 - iv. Passwords must not be revealed or shared on questionnaires or security forms.
 - v. Users must not hint at the format of a password (for example, "my family name").
 - vi. Any user suspecting that his/her password may have been compromised

Cache County School District

Policy Series 6000: Finance and Operations

must report the incident to the Security Officer or technology Help Desk and change the affected district password immediately.

- vii. Through various tools, if the Security Officer or other members of the technology department suspect that a user's account may be compromised:
 - 1. an attempt to contact the user by phone will occur to discuss the possible compromise and possible password resets;
 - 2. at the discretion of the Security Officer, with the goal of maintaining network security, an account may be locked or a password change forced.

C. Authorization

- a. CCSD shall ensure that user access shall be limited to only those specific access requirements necessary to perform the user's job. Where possible, segregation of duties will be utilized to control authorization access.
- b. CCSD shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.
- c. Accounts with elevated privileges will be audited regularly by the Security Officer to determine current access requirements.

D. Accounting

- a. CCSD shall ensure that audit and log files are maintained for at least 90 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.

E. Administrative Access Controls

- a. CCSD shall limit administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.
 - i. The Security Officer may at times choose to permit certain administrative functions to users. These privileges may be revoked at any time as deemed necessary for maintaining system and network security.
- b. Unless specifically required for job functionality, all district owned end user devices should operate under the principle of least privilege e.g. operate as non-administrative limited users.
 - i. Tasks requiring administrative access on end user devices may be resolved by a school IT technician or Help Desk Support.



Cache County School District

Policy Series 6000: Finance and Operations

Incident Management

The Security Officer and Director of Technology are responsible to develop internal IT processes for monitoring and responding to IT-related incidents. These processes will enable notifications of critical events, ensuring rapid response and recovery from internal or external network or system attacks.

Business Continuity

- A. CCSD shall develop and deploy a district-wide business continuity plan, to ensure continuous critical IT services, which should include as a minimum:
 - a. Backup Data: Procedures for performing routine daily/weekly/monthly backups, and for storing backup media at a secured location other than the server room or adjacent facilities.
 - b. Secondary Locations: Identify a backup location, such as another school or district building.
 - c. Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data and restoration of processing at the secondary location.
- B. The Business Continuity/Disaster Recovery Plan shall be private business information due to the security risks that would be present if generally available.

Malicious Software and Patching

- A. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
- B. CCSD shall install, distribute, and maintain Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) on all relevant district-owned equipment, i.e. servers, workstations, and laptops.
 - a. Unauthorized tampering or removal of EDR or XDR software may result in disciplinary action for staff or students, including possible suspension of network and system accounts or termination of employment.
- C. CCSD shall ensure that EDR or XDR protection will include frequent updates and provide real time protection on installed systems.
- D. CCSD shall ensure that all security-relevant software patches are applied on workstations (Mac and PC) within 30 days, and critical patches shall be applied as soon as possible.
- E. CCSD shall ensure that security-relevant software patches are applied regularly based on internal Technology Department secure processes.
- F. Any exceptions to the Malicious Software and Patching section must be approved by the Security Officer.



Cache County School District

Policy Series 6000: Finance and Operations

Internet Content Filtering

- A. In accordance with federal and state law, CCSD shall filter internet traffic for content defined by law as harmful to minors.
- B. CCSD acknowledges that technology-based filters are not always effective at eliminating harmful content and due to this, CCSD uses a combination of technological means and supervisory means to protect students from harmful online content.
- C. In the event that students take devices home, CCSD will provide a technology-based filtering solution for those devices. However, the district relies on parents to provide the supervision necessary to fully protect students from accessing harmful online content.
- D. Students shall be supervised when accessing the internet and using district-owned devices on school property.
- E. Staff, students, and guests shall adhere to the Acceptable Use Policy while using the internet on district properties and on all district-owned devices.

Data Privacy

In conjunction with the Data Governance Procedures and outlined data classifications, CCSD shall ensure that access to employee records shall be limited to only those individuals who have specific access requirements necessary to perform their job duties. Where possible, segregation of duties will be utilized to control authorization access.

Security Audit and Remediation

- A. CCSD shall perform routine security and privacy audits as recommended by the adopted security framework, listed in these procedures, or at minimum completed biennially.
 - a. Including a comprehensive network and system assessment; and
 - b. a phishing component agreed upon between the assessors and the district; and
 - c. a review of the district's progress towards alignment with the approved cyber security framework.
- B. Security audit reports shall be protected business information due to the security implications of disclosure.
- C. The Security Officer shall develop internal remediation plans to address identified lapses or new and emerging cyber security concerns.
- D. Findings will be presented to the Board of Education in a high-level report upon request or after each scheduled assessment is completed.



Cache County School District

Policy Series 6000: Finance and Operations

Employee Disciplinary Actions

Employee disciplinary actions shall be in accordance with applicable laws, regulations and district policies. Any employee found to be in violation may be subject to disciplinary action including termination of employment with CCSD.

Approved by District Administration: May 15, 2025