Cache County School District

Information Technology Security Plan

I. Purpose

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

II. Plan

A. It is the plan of CCSD to support secure network systems, processes, and procedures, and to protect all personally identifiable or confidential information that is stored, on paper or digitally, in district facilities or on district-maintained servers, computers and networks. This plan supports efforts to mitigate threats that may cause harm to the district, its students, or its employees.

B. Data loss or compromises can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be completely preventable.

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

D. This plan and procedure also covers third party vendors/contractors that house or have access to CCSD personally identifiable information. All third party entities will be required to sign the *Restriction on Use of Personally Identifiable or Confidential Information Agreement* before accessing CCSD systems or receiving information.

E. It is the plan of CCSD 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 Governmental Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), and U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.*

F. 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 the Utah Education Network and the Utah State Board of Education. CCSD supports the development and implementation of, and ongoing improvements for, a robust security system of hardware and software that is designed to protect CCSD's data, users, and electronic assets.

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

I. **Sensitive data**: 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.

IV. Security Responsibility

A. CCSD shall appoint an IT Security Officer (ISO) responsible for overseeing district-wide IT security, to include development of district policies and adherence to the standards defined in this document.

V. Training

A. CCSD, led by the ISO, shall ensure that all district employees having access to personally identifiable or confidential information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all district employees.

B. CCSD, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

VI. Physical Security

A. Computer Security

   a. An employee's computer should not be left unattended and unlocked, especially when logged in to sensitive systems or data including student or employee information. Automatic log off, locks and password screensavers should be used to enforce this requirement.

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

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 allowed unescorted access.
  b. 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.

VII. 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 ISO.
   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, WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

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, which is protected by multiple factor authentication systems. Any exception to this plan must be due to a service provider's technical requirements and must be approved by the ISO.

VIII. 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. All server system-level passwords must conform to the *Password Construction Guidelines* posted by the ISO 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.

iv. Passwords must not be revealed or shared on questionnaires or security forms.

v. User 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 must report the incident and change all passwords.

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.

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

IX. Incident Management

A. 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.

X. Business Continuity

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

B. CCSD shall develop and deploy a district-wide business continuity plan 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. As a minimum, backup media must be stored off-site at a reasonably safe distance from the primary server room.

   b. Secondary Locations: Identify a backup processing 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.

XI. Malicious Software

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 spyware and virus protection software on all relevant district-owned equipment, i.e. servers, workstations, and laptops.

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

D. CCSD shall ensure that all security-relevant software patches (relevant workstations and servers) are applied within 30 days, and critical patches shall be applied as soon as possible.

E. All computers must use the relevant district- approved anti-virus solution.

F. Any exceptions to section XI must be approved by the ISO.

XII. 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.

XIII. Data Privacy

A. CCSD considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

B. CCSD 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") and Utah Administrative Code R277-487 ("Student Data Protection Act").*

C. CCSD shall ensure that access to employee records 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.

XIV. Security Audit and Remediation

A. CCSD shall perform routine security and privacy audits as recommended by the district's *Information Security Audit Plan*.

B. District personnel shall develop remediation plans to address identified lapses that conform with the district's *Information Security Remediation Plan Template*.

XV. Employee Disciplinary Actions

A. 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.