Coahoma County School District 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 Coahoma 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. Data loss or compromises can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be completely preventable. This plan supports efforts to mitigate threats that may cause harm to the district, its students, or its employees.

B. 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 administration with relevant information.

C. This plan and procedure also cover 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.

D. It is the plan of CCSD to fully conform with all federal and state privacy and data governance laws.

E. Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. 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.

F. This plan will fully conform with the guidelines of CCSD's Acceptable Use Policy.
G. Best practices will be used to maintain a successful data security program such as outlined in the Data Security Checklist in the Appendix of this plan.

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

CCSD's Technology Director is 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 Technology Director, 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 Technology Director, shall ensure that all students are informed of Cyber Security Awareness.

VI. Physical Security

A. Computer Security
   a. CCSD shall ensure that any user's computer will 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 screen savers 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 method, 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 doors to be opened.

C. 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. 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 Technology Director.

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. 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 Technology Director.

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 structure set by the Technology Director 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 members 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, restoration of processing at the

secondary location, and generation of student and employee listings for ensuring a full head count of all.

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 Technology Director.

XII. Internet Content Filtering

A. In accordance with federal and state law, CCSD shall filter internet traffic for content defined in 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").*
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.
B. District personnel shall develop remediation plans to address identified cyber security issues.

XV. 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 up to and including termination of employment with CCSD.

Appendix

Data Security Checklist

About PTAC

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available at https://studentprivacy.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose

The purpose of this checklist is to assist stakeholder organizations, such as state and local education agencies, with developing and maintaining a successful data security program. A data security program is a vital component of an organizational data governance plan, and involves management of people, processes, and technology to ensure physical and electronic security of an organization's data. A comprehensive security program is critical to protecting the individual privacy and confidentiality of education records. Solutions and procedures supporting data security operations of education agencies should address their unique challenges, including the need to protect personally identifiable information (PII) while maintaining quality, transparency, and necessary access to the data. To ensure that all aspects of a security plan are executed properly, the program should offer clear guidance and tools for implementing security measures. The summary below lists essential components that should be considered when building a data security program. More information on terms discussed in this checklist is available at https://studentprivacy.ed.gov/glossary.

Data Security Checklist

- ❑ **Policy and governance.** Develop a comprehensive data governance plan that outlines organizational policies and standards regarding data security and individual privacy protection. The plan should clearly identify staff responsibilities for maintaining data security and empower employees by providing tools they can use to minimize the risks of unauthorized access to PII. Refer to PTAC's Data Governance Checklist for more information.

- ❑ **Personnel security.** Create an Acceptable Use Policy that outlines appropriate and inappropriate uses of Internet, Intranet, and Extranet systems. Incorporate security policies in job descriptions and specify employee responsibilities associated with maintaining compliance with these policies. Conduct regular checks and trainings to ensure employee understanding of the terms and conditions of their employment. Confirm the trustworthiness of employees through the use of personnel security screenings, policy training, and binding confidentiality agreements.

- **Physical security.** Make computing resources physically unavailable to unauthorized users. This includes securing access to any areas where sensitive data (i.e., data that carry the risk for harm[1] from an unauthorized or inadvertent disclosure) are stored and processed, such as buildings and server rooms. An unlocked server room is an invitation for malicious or accidental damage. Monitor access to these areas to prevent intrusion attempts (e.g., by administering identification badges and requiring staff and visitors to log in prior to entering the premises or accessing the resources).

- **Network mapping**. Network mapping provides critical understanding of the enterprise (servers, routers, etc.) and its connections. Furthermore, network mapping can capture applications and associated data. A robust mapping capability will map the dependencies between applications, data, and network layers, and highlight potential vulnerabilities. There are a number of network mapping tools available.

- **Inventory of assets.** The inventory should include both authorized and unauthorized devices used in your computing environment. These devices are often scanned and discovered by automated programs (continuously searching the internet for vulnerabilities) and if unsecured devices are discovered they can be compromised. Inventorying, when used in conjunction with network mapping, will give your organization a better understanding of the security requirements needed to protect your assets.

- **Authentication.** The ways in which someone may be authenticated fall into three categories: something you know, something you have, or something you are. Two-factor authentication (TFA) combines two of these elements and is more costly, but provides more security. Consider TFA for remote users or privileged "super users." Authentication technologies provide assurance that the person is authorized to access network assets, services, and information.

- **Provide a layered defense.** Employ a "Defense in Depth" architecture that uses a wide spectrum of tools arrayed in a complementary fashion. The most common layers to protect are hosts (individual computers), application, network, and perimeter. There are specific security controls that are suited for use at each of these layers. Relying on a firewall alone to protect your network is never adequate.

- **Secure configurations.** It is a best practice not to put any hardware or software onto your network until it has been security tested and configured to optimize its security. Continuous scanning to ensure system components remain in a secure state is a critical capability that will enhance data security protection. Proactive management of security risks also involves establishing a comprehensive change management program to analyze and address security and privacy risks introduced by new technology or business processes.

- **Access control**. Securing data access includes requiring strong passwords and multiple levels of user authentication, setting limits on the length of data access (e.g., locking access after the session timeout), limiting logical access to sensitive data and resources, and limiting administrative privileges. Role-based access is essential for protecting PII and sensitive data;

[1] Here, harm refers to any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII (NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010 Special Publication 800-122, p. 3-1, 2). Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging).

defining specified roles and privileges for users is a required security procedure. Sensitive data that few personnel have access to should not be stored on the same server as other types of data used by more personnel without additional protections for the data (e.g., encryption).

- **Firewalls and Intrusion Detection/Prevention Systems (IDPS).** A firewall is a device designed to permit or deny network transmissions based upon a set of rules. Firewalls are frequently used to protect networks from unauthorized access, while permitting legitimate communications to pass. An IDPS is a monitoring device that is designed to detect malicious activity on the network. Although some automatically take remediation action, most report suspicious activity to a central monitoring point for further analysis.

- **Automated vulnerability scanning.** When new vulnerabilities (to hardware, operating systems, applications, and other network devices) are discovered, hackers immediately scan networks for these vulnerabilities. Scanning your network and systems on a regular basis will minimize the time of exposure to known vulnerabilities.

- **Patch management.** Patch management is the process of using a strategy and plan for the testing and roll out of software updates and patches on a regular basis. The plan should address how patches will be applied to which systems at a specified time. A patch is a piece of code that protects computers and applications by updating the security state against new threats or vulnerabilities. Used in conjunction with vulnerability scanning, the enterprise can quickly shut down any vulnerability discovered.

- **Shut down unnecessary services.** Each port, protocol, or service is a potential avenue for ingress into your enterprise. A best practice, which should be part of a secure configuration, should include shutting down all services and ports that are not required in your computing environment. A secure enterprise will continually monitor for the use of unapproved ports, protocols or services.

- **Mobile devices.** When sensitive data are stored on servers or on mobile devices, such as laptops or smart phones, the data should be encrypted. There are far too many examples of mobile devices being lost or stolen and the subsequent exposure of the sensitive information stored on those devices in the public domain.

- **Emailing confidential data.** Consider the sensitivity level of the data to be sent over the email. Emailing unprotected PII or sensitive data poses a high security risk. It is recommended that organizations use alternative practices to protect transmissions of these data. These practices include mailing paper copies via secure carrier, de-sensitizing data before transmission, and applying technical solutions for transferring files electronically (e.g., encrypting data files and/or encrypting email transmissions themselves).

- **Incident handling.** When an incident does occur it is critical to have a process in place to both contain and fix the problem. Procedures for users, security personnel, and managers need to be established to define the appropriate roles and actions. Outside experts may be required to do a forensics investigation of the incident, but having the correct procedures in place initially will minimize the impact and damage.

- **Audit and compliance monitoring.** Audits are used to provide an independent assessment of your data protection capabilities and procedures (see Data Stewardship: Managing Personally

Identifiable Information in Electronic Student Education Records) and should be performed periodically. Auditors that are familiar with Family Educational Rights and Privacy Act statutory and regulatory requirements can further assist you in determining whether your systems are in compliance.