Note: For information regarding retention and security of records containing criminal history record information, as well as procedures for reporting security incidents regarding such information, see DBAA. For information on cybersecurity for Texas school districts, see the Texas Education Agency's Cybersecurity Tips and Tools[1] and the Texas Department of Information Resources[2] page on Information Security. Data Privacy and Cybersecurity Services[3] information can be found on the Texas Association of School Boards website.

Cybersecurity Plan

Dustin Hardin, Chief Technology Officer will develop and implement a plan to increase cybersecurity and lessen the District's vulnerability to unauthorized efforts to access District data. These efforts will include both technological safeguards, such as password complexity requirements and regular data backups, and training for users in recognizing and reporting activity aimed at gaining unauthorized access, such as phishing and spoofing. The District's plan must not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources (DIR). See CQB(EXHIBIT) Data Breach Prevention and Response Plan.

Plan Review and Coordination

The cybersecurity plan will be reviewed at least annually and be properly coordinated with the District's other plans, including the multi-hazard emergency operations plan, disaster recovery plan, and information management or security plans.

Cybersecurity Coordinator

The Superintendent has designated the following person as the cybersecurity coordinator:

Dustin Hardin
Chief Technology Officer
dhardin@ccisd.net
(281) 284-0401

The cybersecurity coordinator for the District's cyberinfrastructure will:

1. Serve as the liaison between the District and the Texas Education Agency (TEA);
2. Report to TEA, as required by law, and other required authorities any breach of the District's system security;
3. Provide notice to a parent of or person standing in parental relation to an enrolled student about any attack or incident for

which reporting was required by law and that involved the student's information;

4. Verify and report on compliance with staff training requirements as required by the Board; and

5. Preserve necessary records for audit purposes and assist in responding to audits to ensure compliance with law and policy.

Training

The Board delegates to the Superintendent the authority to select or develop a cybersecurity training program to fulfill the District's cybersecurity training requirements.

District employees who have access to District computer systems or databases will be required to annually complete the District's designated cybersecurity training program.

Any new employee who has access to District computer systems or databases hired during the school year will be trained within 15 school days following the employee's start of employment. All District employees will be provided information on the District's cybersecurity policies and program.

Any agent, consultant, volunteer, or other authorized user who has access to District computer systems or databases will be required to annually complete the District's designated cybersecurity training program in accordance with relevant user agreements.

Training Verification and Audits

All training requirements will be verified and reported to the DIR by the cybersecurity coordinator.

If an employee does not complete the required annual training, disciplinary action may be taken.

---

[1] Texas Education Agency's Cybersecurity Tips and Tools: https://www.texasgateway.org/resource/cybersecurity-tips-and-tools.
[2] Texas Department of Information Resources: https://dir.texas.gov/View-About-DIR/Information-Security/Landing.aspx
[3] Texas Association of School Boards' Data Privacy and Cybersecurity Services: https://www.tasbrmf.org/member-service-center/risk-solutions/special-risk-services/data-privacy-and-cybersecurity.aspx