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 DIR's Required Cybersecurity Training Reporting Form for Local Governments.[2] Data Privacy and Cybersecurity Services[3] information can be found on the Texas Association of School Boards website.

Cybersecurity Plan

Executive Director, Cybersecurity & IT Operations 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).

Plan Review and Coordination

The cybersecurity plan will be reviewed periodically, but no less frequently than every three years, and be properly coordinated with the District's other plans, including the multi-hazard emergency operations plan, disaster recovery plan, security plans, and safety and security audit.

Cybersecurity Coordinator

The Superintendent has designated the following person as the cybersecurity coordinator and submitted their information to TEA via the AskTED[4] portal:

Name *(print)*: Troy Neal

Position: Executive Director, Cybersecurity & IT Operations

Email: Troy.neal@springbranchisd.com

Phone number: 713-251-1416

The cybersecurity coordinator for the District's cyberinfrastructure will:

1. Serve as the liaison between the District and other entities or individuals involved in the District's responses to potential incidents, such as the Texas Education Agency (TEA), the attorney general, federal and state law enforcement, and/or affected individuals;

2. Obtain annual cybersecurity training required by Government Code 2054.5191;

3. Coordinate and support response to incidents that meet the legal definition for a breach of system security [see CQB(LEGAL)], including notifying or assisting with notification to TEA or, if applicable, the entity that administers the anonymous cyberattack/incident information-sharing system established by TEA for participating schools and the state, if a breach that meets the legal definition involves sensitive, protected, or confidential student data;

4. Coordinate or issue notification 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;

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

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

Training Program

In accordance with the Board's authorization through Board policy, the Superintendent has selected the following cybersecurity training program to fulfill the District's cybersecurity training requirements: district developed and DIR certified program.

Training Requirements

Board members, district employees and non-employees who are issued a district device or need access to the district's network or email system complete their required duties will be required to complete the District's designated cybersecurity training program in accordance with the District's locally determined training schedule established in coordination with the District's cybersecurity coordinator.

In addition to required cybersecurity training under law, the District at its own discretion may require cybersecurity training for additional individuals as determined necessary.

Exceptions to Training Requirements

By law, cybersecurity training will not be required for employees and officials who have been:

- Granted military leave;
- Granted leave under the federal Family and Medical Leave Act of 1993 (29 U.S.C. Section 2601 et seq.);

- Granted leave related to a sickness or disability covered by workers' compensation benefits, if that employee no longer has access to the District's database and systems;
- Granted any other type of extended leave or authorization to work from an alternative work site if that employee no longer has access to the District's database and systems; or
- Denied access to the District's computer system or database for not complying with cybersecurity training requirements.

Cybersecurity training requirements will resume once an employee or official returns from leave, as applicable.

All District employees will be provided information on the District's cybersecurity policies and program.

Training Verification and Audits

In accordance with the Board's authorization through Board policy, the Superintendent will verify and report compliance with the staff training requirements in accordance with DIR guidelines.

Audits regarding staff training will be completed by the cybersecurity coordinator to ensure compliance with the cybersecurity training requirements.

The form to report the completion of cybersecurity training by employees, Cybersecurity Training Certification for Local Governments,[5] can be found on DIR's website.

Determination of Noncompliance and System Access

The Board has designated the Superintendent or designee to make determinations regarding training compliance and approve denials of access to District computers and/or computer systems and databases.

Any District employee or Board member who fails to meet training requirements under law or as required by the District and does not qualify for a training exception may be determined to be noncompliant and may be subject to denial or reduction of access to the District's computers and/or computer systems and databases. Noncompliant employees may be subject to disciplinary action.

Incident Response

The Superintendent has designated the cybersecurity coordinator to lead the incident response team when necessary to respond to a cybersecurity incident and ensure the District's compliance with the District's incident response plan.

---

[1] Texas Education Agency's Cybersecurity Tips and Tools: https://www.texasgateway.org/resource/cybersecurity-tips-and-tools.

[2] Texas Department of Information Resources-Required Cybersecurity Training Reporting Form for Local Governments: https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=232
[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
[4] AskTED Portal: https://tea4avholly.tea.state.tx.us/tea.askted.web/forms/home.aspx
[5] DIR, Cybersecurity Training Certification for Local Governments: https://dircommunity.force.com/SecurityTrainingVerification/s/CybersecurityTrainingCertification