Data Breach Prevention and Response Plan

The District's Executive Director, Cybersecurity & Technology Operations is responsible for periodically reviewing this plan and updating the guidelines as needed.

Security Breach Prevention

Maintain and update the breach response team contact list: Check that the contact information is accurate. Redistribute the updated list as needed.	Quarterly
Review the District's information systems and keep records identifying locations and systems that house personally identifiable information and other sensitive information: Ensure that confidential information is stored on a secure server that is accessible only with a password or other security protection. Keep and update records of all persons with access to District servers through personal or District-issued mobile devices and laptops and ensure that each device is password-protected and encrypted, as applicable. Ensure that District-maintained, cloud-based applications that use or maintain student or staff data, including criminal history record information, are compliant with the Family Educational Rights and Privacy Act (FERPA), the Children's Internet Protection Act (CIPA), and other federal and state law. Review the District's Software Approval Process for requests from professional staff members for use of additional online educational resources, including review of the terms of service or user agreements, to ensure compliance with District standards and applicable law and coordinate with the Compliance Officer as necessary.	Annually
Compile a list of third-party vendors with access to sensitive information, including the types of information and uses of the information. Issue a reminder to all relevant parties to secure sensitive paper records; password-protect records stored on thumb drives, external hard drives, and laptops; and dispose of records in accordance with the district's records retention requirements.	Annually

Review third-party vendor contracts: Coordinate with the Procurement Office to ensure that vendor contracts for cloud-based applications that use or maintain student or staff data are compliant with FERPA, CIPA, and other federal and state law. Ensure that contracts include breach notification.	Ongoing
In conjunction with the records retention officer, ensure that archived data meets industry standards and legal requirements for secure storage and review data storage and disposal protocols.	Annually
Update local security measures, including: Service accounts and system passwords, including a list of District employees with administrator access to information systems; Endpoint protection software; Firewalls; Data backup procedures; Data encryption procedures; and Data and records disposal best practices.	Ongoing
Monitor systems for packet loss.	Continually
Conduct trainings with students, staff members, Board members, and others as needed on privacy and security awareness and District protocols for storing, accessing, retaining, and disposing of records.	Annually

Incident response team

Name	Position	Contact Information	Responsibility during Breach
Troy Neal	Cybersecurity Coordinator designee and Technology Executive Director (if electronic records)	Phone: 713-251-1416 Email: Troy.neal@springbranchisd.com	Notify the team and Assoc. Supt., Technology. Identify the affected records. Evaluate for further notification and engagement.
Matthew Barile	Security Engineer	Phone: 713-251-1402 Email: matthew.barile@springbranchisd.com	Notify the Engineering team. Identify the affected records.
Lawanda Coffee	Records Management Officer (if paper records)	Phone: 713-251-2267 Email: lawanda.coffee@springbranchisd.com	Notify the Procurement team. Identify the affected records.
Melissa Wiland	Director of Communications	Phone: 713-251-2469 Email: melissa.wiland@springbranchisd.com	Coordinate the notification and communications plan.
To Be Determined (based on incident specifics)	Outside Counsel	To Be Determined (based on incident specifics)	Analyze the legal implications and advise the team regarding litigation risks and notification requirements.
Christina Masick	Associate Supt., Technology	Phone: 713-251-2249 Email: christina.masick@springbranchisd.com	Notify Superintendent and Senior Staff, as necessary

Vendor list

The following outside vendors contract with the District for cloud-based (online) or other technology applications that have access to potentially sensitive student or staff information.

Name of vendor: Skyward	Vendor contact information: Skyward main number 800-236-7274 Skyward support number 800-236-0001
Is vendor considered a "school official" for purposes of access to student records? Yes	
Type of data: Student Records and grade book	Use of data/service provided: Student information system
Contract owner: Mark Maxwell	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: Tyler Technologies (MUNIS)	Vendor contact information: 800-772-2260
Is vendor considered a "school official" for purposes of access to student records? No; system does contain sensitive staff information	
Type of data: Employee Records/Financials	Use of data/service provided: Enterprise resource management
Contract owner: Mark Maxwell	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: Instructure Canvas	Vendor contact information: 1-800-203-6755
Is vendor considered a “school official” for purposes of access to student records? Yes	
Type of data: Directory information, grades, and tests	Use of data/service provided: Learning Management System
Contract owner: Annie Wolfe	Date contract last reviewed for security compliance: 2/5/2022

Name of vendor: Frontline Education (Appli-track/AESOP)	Vendor contact information: 800-365-0114
Is vendor considered a “school official” for purposes of access to student records? No; system does contain sensitive staff information	
Type of data: Potential employee data and staff absence data	Use of data/service provided: Applicant tracking and employee absence tracking
Contract owner: Allison Tennyson	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: SchoolCity	Vendor contact information: 949-656-3133
Is vendor considered a “school official” for purposes of access to student records? Yes	
Type of data: Employee Records/Financials	Use of data/service provided: Student assessment solution
Contract owner: Keith Haffey	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: SuccessEd	Vendor contact information: 214-613-1546
Is vendor considered a “school official” for purposes of access to student records? Yes	
Type of data: Student Records	Use of data/service provided: Special Education Data Management
Contract owner: DeAnne Baker	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: eShars	Vendor contact information: 512-463-6639
Is vendor considered a “school official” for purposes of access to student records? Yes	
Type of data: Student records	Use of data/service provided: Medicaid reimbursement program
Contract owner: DeAnne Baker	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: Primero	Vendor contact information: 866-442-6030
Is vendor considered a “school official” for purposes of access to student records? Yes	
Type of data: Student Records	Use of data/service provided: Food Service/POS system
Contract owner: Michael Francis	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: MySchoolBucks	Vendor contact information: 855-832-5226
Is vendor considered a “school official” for purposes of access to student records? Yes	
Type of data: Student Records	Use of data/service provided: Online payment system for student fees
Contract owner: David Bender	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: SNAP	Vendor contact information: 800-889-7627
Is vendor considered a “school official” for purposes of access to student records? Yes	
Type of data: Student Medical records	Use of data/service provided: Nurse medical record system
Contract owner: Connie Hamon	Date contract last reviewed for security compliance: 7/2/2022

Name of vendor: Spindlemedia Tax Office	Vendor contact information: 972-538-3750
Is vendor considered a “school official” for purposes of access to student records? No	
Type of data: Banking information	Use of data/service provided: Tax records
Contract owner: Elizabeth Ruiz	Date contract last reviewed for security compliance: 7/2/2022

Responding to a Potential Breach

Note: For a breach involving criminal history record information, see DBAA.

Upon notification that a potential breach may have occurred, the cybersecurity coordinator will immediately notify the incident response team and:

- ☐ Validate the facts that indicate a potential data breach;
- ☐ Determine the scope of the potential breach;
- ☐ Notify the District's data breach coverage provider;
- ☐ Notify law enforcement, if needed;
- ☐ Notify the attorney general, if a breach incident meets the legal requirement to notify the attorney general and involves at least 250 Texas residents [See CQB(LEGAL)];
- ☐ Notify affected individuals, if a breach incident meets the legal requirement to notify individuals, in accordance with law [see CQB(LEGAL)] and Board policy;
- ☐ Notify TEA and parents, if a breach incident meets the legal requirement to notify TEA, in accordance with law involving sensitive, protected, or confidential student data [See CQB];
- ☐ Determine whether there is a need for outside resources, such as privacy counsel, digital forensics examiners, credit monitoring services, and the like;
- ☐ Coordinate the incident response team and ensure that the team handles responsibilities in accordance with the nature and severity of the incident, including determining whether notification of affected individuals is appropriate and, if so, how best to provide the notification;
- ☐ Create, gather, and maintain all documents related to the incident; and
- ☐ Analyze information to determine the cause of the incident (internal cause, third-party breach, etc.) and take measures to address and remediate.