Springfield Public Schools
Written Information Security Program

I. Objectives

The Springfield Public Schools ("SPS") developed this comprehensive written information security program ("Program") to create effective administrative, technical, and physical safeguards for the protection of personal information as defined below ("Personal Information"), and to comply with SPS's obligations under 201 C.M.R. 17.00 and other applicable law ("Regulations"). The Program sets forth SPS's policy for accessing, collecting, storing, using, transmitting, and protecting records containing Personal Information.

II. Scope

All SPS employees and independent contractors are subject to this Program.

This Program applies to any records that contain Personal Information and, to the extent it is practicable, reasonable, and feasible, all other sensitive information which may include Student Education Records and Personnel Records in any format and on any media, whether in electronic or paper form.

For purposes of this Program, "Personal Information" means a first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

For purposes of this Program, Student Education Records are records directly related to the student – and as defined by the Family Educational Rights and Privacy Act (FERPA) and as defined further by 603 CMR 23.02 – and maintained by the Springfield Public Schools and parties acting on behalf of the Springfield Public Schools.

For purposes of this Program, Personnel Records are records directly related to an individual employee or former employee of the Springfield Public Schools and maintained by the Springfield Public Schools and parties acting on behalf of the Springfield Public Schools for legitimate business purposes and in compliance with state and federal regulations.

This Program does not apply to information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

This Program protects employee, student, and customer records containing Personal Information, whether they are held in paper or electronic form. The Program is appropriate to the SPS's size, scope, and business, its available resources, and the amount of Personal Information maintained by SPS.

III. Program

A. Administrative Safeguards

1. **Designation of Responsible Person:** The Springfield Public School's Chief Information Officer, head of the Office of Information, Technology, and Accountability, is the "Information Security Coordinator." The Information Security Coordinator is responsible for overseeing the administrative aspects of the Program, including training, annual review of the Program, incident reporting, and any required risk assessments.

   A Data Security Team will participate in the regular review of this Program and as the Incident Response Team. The Data Security Team will, at a minimum, include the following members.
   - **i.** Chief Information Officer
   - **ii.** Chief Financial Officer or designee
   - **iii.** Chief of Human Resources or designee
   - **iv.** Chief of Parent and Community Engagement or designee
   - **v.** Director of Information Management or designee
   - **vi.** Director of Technology Operations or designee

2. **Identification of Records Containing Personal Information:** Personal Information, Student Education Records, and Personnel Records are contained in paper, electronic, and other records, computing systems, and storage media, including laptops and portable devices, as outlined in Appendix A.

3. **Procedures for Minimizing Risks to Personal Information:** The amount of Personal Information, Student Education Records, and Personnel Records kept by the SPS will be limited to that which is reasonably necessary to accomplish its legitimate business purposes, or to comply with state or federal regulations. To that end, the SPS has the following policies that dictate when and how records containing Personal Information, Student Education Records, and Personnel Records will be retained, accessed, transported, or destroyed.
   - **i. Access:** Access to Personal Information, Student Education Records, and Personnel Records will be limited to those persons who have a need to know such information in order to accomplish their job functions. For example, employee personnel files are stored electronically in a cloud-based storage location and access is restricted via secure password and role-based permission to authorized members of the Human Resources and IT Departments.
   - **ii. Transport:** SPS's policy on transporting records containing Personal Information, Student Education Records, and Personnel Records outside the main business premises or between locations is as follows: print records will

not leave the business premises of SPS except when being transported from one SPS location to another by authorized SPS personnel; and, electronic records will not be transported via portable media (i.e. portable hard drives, flash drives, etc.) without password-protected encryption of the portable media.

iii. **Transmission:** Leaving and retaining voice mail messages containing Personal Information is prohibited. Except as required by state or federal authority, transmission of Personal Information by fax is prohibited. Transmission of Personal Information, Student Education Records, and Personnel Records via paper records outside of SPS must be done with reasonable precaution to prevent unauthorized disclosure. Transmission of Personal Information in electronic form outside of SPS, unless encrypted, is prohibited.

iv. **Retention:** Storage of records containing Personal Information, Student Education Records, and Personnel Records will be limited to the amount reasonably necessary to accomplish SPS's legitimate business purposes and consistent with state and federal regulations. For example, employment applications for staff hired by the Springfield Public Schools will be retained for 20 years after the termination of employment per state regulations.

a. Appendix A contains a list of records with PII, Student Education Records, and Personnel Records kept by the Springfield Public Schools with timelines for retention and destruction.

v. **Destruction of Records Containing Personal Information:** All paper records containing Personal Information to be disposed of must be shredded. Electronic records containing Personal Information will be disposed of by destroying or erasing the records so that Personal Information cannot practicably be read or reconstructed.

4. **Risk Assessment:** The Information Security Coordinator must identify and assess reasonably foreseeable internal and external risk to the security and confidentiality of Personal Information, Student Education Records, and Personnel Records maintained by the SPS, including employee compliance with this Program and the ability to detect and prevent security system failures, and must revisit such assessments whenever there is a material change in business practices that may impact the security or integrity of Personal Information. The Information Security Coordinator has identified the following examples of risks to the security and confidentiality of Personal Information, Student Education Records, and Personnel Records maintained by the SPS.

i. Internal Risks

a. Employee error through inadvertently granting access to SPS systems through responding to a phishing email
b. Employee error through inadvertent disclosure of a password
c. Employee error through not keeping paper records on SPS premises or not securing paper records when not in use

d. Employee error through failure to follow policy regarding encrypted transmission of electronic records outside SPS

ii. External Risks

a. Hacker using malware/virus to expose vulnerability in unpatched software on a server

b. Hacker using malware/virus/phishing attack to gain control of an endpoint (laptop, desktop, or phone) and then accessing other endpoints or servers via the network

Appendix B is SPS' Risk Management Plan, outlining potential risks to, and associated risk mitigation strategies for, the security and confidentiality of Personal Information, Student Education Records, and Employee Records maintained by SPS.

5. **Employee Training:** Employees (and, as applicable, and on an as-needed basis, independent contractors) will receive the following training concerning the handling and protection of Personal Information, Student Education Records, and Employee Records.
   - **i.** All Employees – will annually complete a training module covering, at minimum, the Staff Technology Acceptable Use and Electronic Data Security Policy for staff, protection of sensitive information, the protection of Student Education Records under FERPA, and practices for electronic security including password practices and phishing email awareness.
   - **ii.** Employees with Regular Access to Personal Information – will annually complete an additional training module on this WISP and practices and procedures for handling, storage, transmission, and disposal of paper and electronic records.

6. **Employee Discipline:** Violation of this Program will result in disciplinary action, up to and including termination of employment.

7. **Terminated Employees:** Employees' and/or independent contractors' physical and electronic access to Personal Information records, Student Education Records, and Personnel Records will be terminated upon their termination from employment or the termination of their contract, including, if applicable, immediate deactivation of their online accounts and passwords.

8. **Evaluation of Safeguards and Monitoring of the Program**: Based on his/her knowledge of the risks listed above, the Information Security Coordinator will evaluate the effectiveness of current safeguards and monitor the effectiveness of the Program at least quarterly. That evaluation, at a minimum, will involve the Information Security Coordinator certifying that the Program reasonably protects against unauthorized access to or use of Personal Information, Student Education Records, and Personnel Records that may result in substantial harm or inconvenience to any consumer, student, or employee, as well as a brief description of any additional safeguards or updates in the past year added to adapt the Program to novel or growing internal and external threats

to the security or confidentiality of records. Please see Appendix C, Periodic Evaluation of Program's Safeguards, attached.

9. **Oversight of Service Providers:** Before retaining a third-party service provider who will have access to Personal Information, Student Education Records, or Personnel Records, SPS will take reasonable steps to determine whether the prospective third-party service provider is capable of maintaining appropriate security measures to protect records consistent with this policy and state and federal regulations. Reasonable due diligence may include discussions with the prospective third-party service provider's personnel, review of the prospective third-party service provider's written information security program, and review of the third-party service provider's computer security system.

   Any contracts with third-party service providers who will have access to Personal Information will contain a provision requiring the third-party service provider's capability to implement and maintain appropriate security measures to protect Personal Information.

   Any third-party service provider granted access to Personal Information, Student Education Records, or Personnel Records through an SPS-provided account will agree with the terms of this policy and the Springfield Public Schools' Acceptable Use and Data Security Policy for Staff, available at the following website: https://www.springfieldpublicschools.com/departments/administration/district_policies.

10. **Internal Reporting:** Employees and independent contractors of SPS are encouraged to report to the Information Security Coordinator any activity or conduct which may pose a risk to the security and confidentially of Personal Information, Student Education Records, or Personnel Records.

    If an employee or independent contractor of SPS learns or becomes aware of a known or suspected breach of security, including but not limited to the unauthorized acquisition or unauthorized use of Personal Information, the individual must immediately notify the Information Security Coordinator via email. In addition, the District will provide a means for the anonymous reporting of suspected breaches of security to the Information Security Coordinator.

11. **Incident Response Procedure:** In the event that the SPS experiences a suspected or confirmed breach of security, where a breach of security is defined as "the unauthorized acquisition or unauthorized use of unencrypted data containing Personal Information, Student Education Records, or personnel record, or the unauthorized acquisition or unauthorized use of encrypted electronic data containing Personal Information, Student Education Records, and Personnel Records and the confidential process or key capable of decrypting that information," it will follow an incident response plan.

The incident response plan will include, at minimum, notification to the Superintendent of Schools, Chief Financial Officer, and Chief of Human Resources; meeting of the data security team to mitigate the breach to the extent possible, investigate the source of the breach, and propose steps to improve security; notification of impacted students, staff, or consumers consistent with state and federal regulations; and, completion of a post-incident review of events and actions taken to improve the security of Personal Information, Student Education Records, and Personnel Records (see form in Appendix D). Incident response is documented using the form in Appendix E.

B. Physical Safeguards

1. **Storage of Records in Locked Facilities, Areas, or Containers:** Paper records containing Personal Information, Student Education Records, or Personnel Records will be stored in locked facilities, areas, or containers.

2. **Restriction on Physical Access to Records Containing Personal Information:** The SPS restricts physical access to records containing Personal Information in the following manner:
    - **i.** Access to locked facilities, areas, and containers is only provided to employees or independent contractors who need access to this information to perform their job functions.
    - **ii.** Any keys to locked facilities, areas, and containers are received back from employees or independent contractors immediately upon termination of employment, contract, or need for access.

C. Technical Safeguards

To protect electronically-stored Personal Information, Student Education Records, and Personnel Records, and to the extent technically feasible, the SPS has the following safeguards in place.

1. **Access Control Measures**: SPS restricts access to electronic records and files containing Personal Information, Student Education Records, and Personnel Records to employees and/or independent contractors who need to know this information to perform their job functions.

2. **Unique Identifiers:** SPS assigns unique identifications and passwords (which are not default, vendor-supplied passwords) to each employee, and/or independent contractor with access to any SPS computer system.

3. **Secure User Authentication Protocols:** SPS has in place secure user authentication protocols, including:
    - **i.** Protocols for assigning and controlling user IDs and other identifiers

ii. Protocols for assigning a second, independent user ID and secure password, separate from a user's standard account password to users for purposes of accessing Personal Information stored on electronic locations with higher levels of security
iii. A reasonably secure method of assigning and selecting secure passwords
iv. A practice of keeping passwords in a location and format that does not compromise the security of the data they protect
v. Restricting access to Personal Information to active users and active user accounts with protocols to disable access upon employee termination or the end of an independent contractor's contract
vi. Blocking access to online resources after multiple unsuccessful attempts to gain access

4. **Password Policy:** SPS requires that current computer or network passwords be a minimum of 8 characters and include three of the following: upper case letters, lower case letters, numbers, and special characters. Passwords are required to be changed periodically. When possible, and for access to Personal Information, multi-factor authentication protocols are used to require employees and independent contractors with SPS accounts to verify their identity when logging into their account from an unfamiliar device or location.

5. **Encryption in Transit:** To the extent technically feasible, all Personal Information, Student Education Records, and Personnel Records transmitted wirelessly across public networks are encrypted.

6. **Encryption at Rest:** To the extent technically feasible, all Personal Information stored on laptops or other portable devices is encrypted.

7. **Monitoring:** SPS has monitoring in place to alert it to the occurrence of unauthorized use, access to, storage, or transmission of Personal Information.

8. **Firewall Protection:** On any of its computer systems containing Personal Information, Student Education Records, and Personnel Records that are connected to the Internet, SPS has reasonably up-to-date firewall protection and operating system security patches to maintain the integrity of the Personal Information.

9. **Malware Protection:** SPS has reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions.

IV. Program History

This WISP is effective as of October 28, 2021.

It was originally published on October 28, 2021, reviewed on the dates noted in the attached

Appendix A – Inventory of Personal Information, Student Education Records, and Personnel Records

The inventory of Personal Information, Student Education Records, and Personnel Records maintained by the Springfield Public Schools, including information on how the information is stored, secured, and accessed is maintained and regularly updated by the Information Security Coordinator. Because of the length, complexity, and confidentiality of this information, it is not attached to this Program for public dissemination.

Appendix B – Risk Management Plan

The Risk Management Plan – documenting known risks to information security and steps taken to mitigate those risks – is maintained and regularly updated by the Information Security Coordinator consistent with this Program. Because of the confidentiality of this information, it is not attached to this Program for public dissemination.

Appendix C – Periodic Evaluation of Program Safeguards Form

Name of Information Security Coordinator:	
Date of Periodic Evaluation:	

What changes, if any, have been made to the Program since the last reporting period?

What changes, if any, are underway or in process, but not yet fully implemented and when will they be fully implemented?

Do the safeguards of the Program provide a reasonable level of security? (YES or NO)	

Appendix D – Post-Incident Review Form

Name of Person Completing Form:	
Date of Incident:	

Describe the incident, including the date and time the incident began, the date it was discovered, and the type and quantity of Personal Information or other sensitive information that was involved.

Was the incident caused by an internal or external threat, or a mix of the two?

Did your detection and response process and procedures work as intended? If not, where did they not work? Why did they not work?

How could monitoring procedures be improved to detect an intrusion or incident earlier in the process?

What are some improvements to procedures and tools that would aid in the response process? For example, would changing the placement of firewalls limit the scope of similar, future incidents?

What are some actions you took and procedures you followed that helped to contain or mitigate the potential scope of the Personal Information or other sensitive information impacted by this incident? What are any additional improvements you could make to enhance your ability to contain the scope of a similar incident?

What changes should be made to policies and procedures that will allow the response and recovery processes to operate more smoothly?

Appendix E – Incident Response Plan

1) Alert Information Security Officer (ISO).

2) ISO Activates the Data Security Team, Technical Professionals, and notifies the Superintendent.

3) Technical Professionals contain the breach and preserve evidence of what occurred, engaging vendors as necessary.

4) ISO contacts legal who can i) determine if incident is a reportable breach ii) retain a forensic expert to investigate the breach, if necessary; and, iii) coordinate other contacts.

5) ISO or designee contact Law Enforcement, as applicable.

- Multi-State Information Sharing and Assistance Center
- Massachusetts State Police
- Federal Bureau of Investigation

6) Technical Professionals, working with Law Enforcement or forensic expert if necessary, investigate the cause and scope of the breach.

7) ISO in collaboration with legal, make required breach notifications.

8) ISO completes incident review with Data Security Team.

9) Data Security Team updates Written Information Security Program based on review.

Incident Response Plan Contact Template

The Data Security Team's members will each have copies of the updated incident response contact template illustrated below.

Name	Role	Mobile Phone	Email	Backup
	Info Sec Officer			
	Data Sec Team			
	Tech Professional			
	Superintendent			
	Asst Super			
	Legal Counsel			
	Communications			