Solomon Schechter Day School Written Information Security Program

1.0 Policy Statement

The Solomon Schechter Day School (“SSDS”, or the “School”) Written Information Security Program (“WISP”) is intended as a set of comprehensive guidelines and policies designed to safeguard all confidential and restricted data maintained at the School, and to comply with applicable laws and regulations on the protection of Personal Information and Nonpublic Financial Information, as those terms are defined below, found in records and in systems owned by the School.

2.0 Overview & Purpose

This WISP was implemented to comply with regulations issued by the Commonwealth of Massachusetts entitled “Standards For The Protection Of Personal Information Of Residents Of The Commonwealth” [201 Code Mass. Regs. 17.00], and by the Federal Trade Commission [16 CFR Part 314], and with our obligations under the financial customer information security provisions of the federal Gramm-Leach-Bliley Act (“GLB”) [15 USC 6801(b) and 6805(b)(2)].

In accordance with these federal and state laws and regulations, SSDS is required to take measures to safeguard personally identifiable information, including financial information, and to provide notice about security breaches of protected information at the school to affected individuals and appropriate state agencies.

SSDS is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work or study at the School. SSDS has implemented a number of policies to protect such information, and this WISP should be read in conjunction with these policies that are cross-referenced at the end of this document.

The purposes of this document are to:

- Establish a comprehensive information security program for the School with policies designed to safeguard sensitive data that is maintained by the School, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.
3.0 Scope

This Program applies to all SSDS employees, whether full- or part-time, including faculty, administrative staff, contract and temporary workers, hired consultants, interns, as well as to all other members of the School community (hereafter referred to as the “Community”). This program also applies to certain contracted third-party vendors (see section 4.6 for further information). The data covered by this Program includes any information stored, accessed or collected at the school or for school operations. This WISP is not intended to supersede any existing SSDS policy that contains more specific requirements for safeguarding certain types of data, except in the case of Personal Information and Nonpublic Financial Information, as defined below. If such policy exists and is in conflict with the requirements of this WISP, the other policy takes precedence.

3.1 Definitions

Data

For the purposes of this document, data refers to information stored, accessed or collected at the school about members of the school community.

Data Custodian

A data custodian is responsible for maintaining the technology infrastructure that supports access to the data, safe custody, transport and storage of the data and provide technical support for its use. A data custodian is also responsible for implementation of the business rules established by the data steward.

Data Steward

A data steward is responsible for the data content and development of associated business rules, including authorizing access to the data.

Personal Information

Personal Information (“PI”), as defined by Massachusetts law (201 CMR 17.00), is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver’s license number or state-issued identification card number; or
- Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person’s financial account, with or without any required security code, access code, personal identification number, or password.

For the purposes of this Program, PI also includes passport number, alien registration number or other government-issued identification number.

Nonpublic Financial Information
The GLB Act (FTC 16 CFR Part 313) requires the protection of “customer information”, that applies to any record containing nonpublic financial information (“NFI”) about a student or other third party who has a relationship with the school, whether in paper, electronic or other form, which is handled or maintained by or on behalf of the school. For these purposes, NFI shall include any information:

- A parent or other third party provides in order to obtain a service from the School;
- About a student or other third party resulting from any financial transaction with the School; or
- Otherwise obtained about a student or other third party in connection with providing a service to that person.

Examples of NFI include:

1. Information a consumer provides to you on an application to obtain a product or service;
2. Account balance information, payment history, overdraft history, and credit or debit card purchase information;
3. The fact that an individual is or has been one of your customers or has obtained a product or service from you;
4. Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
5. Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
6. Any information you collect through an Internet “cookie” (an information collecting device from a web server); and
7. Information from a consumer report.

3.2 Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

Confidential

Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to SSDS or the Community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

Confidential data includes data that is protected by the following federal or state laws or regulations: 201CMR17.00 (Mass Security Regs), 16 CFR 313 (Privacy of Consumer Financial Information), the Federal Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the FTC’s Red Flag Rules. Information protected by these laws includes, but is not limited to, PI, NFI and Protected Health Information (PHI).
Restricted

Restricted data refers to all other personal and institutional data where the loss of such data could harm an individual’s right to privacy or negatively impact the finances, operations or reputation of the School. Any non-public data that is not explicitly designated as Confidential should be treated as restricted data.

Restricted data includes data protected by the Family Educational Rights and Privacy Act (FERPA), referred to as student education records. This data also includes, but is not limited to, donor information, research data on human subjects, intellectual property (proprietary research, patents, etc.), school financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Restricted data should be limited to access by individuals who are employed by the School and who have legitimate reasons for accessing such data, as governed by FERPA, or other applicable law or school policy. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Public (or Unrestricted)

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to the School or members of the SSDS community. Any data that is not classified as Confidential or Restricted should be considered Public data.

4.0 Policy

4.1 Responsibilities

All data at the School is assigned a data steward according to the constituency it represents. Data stewards are responsible for approval of all requests for access to such data. The data steward for each constituency group are designated as follows:

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Data Steward*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty</td>
<td>Director of Finance &amp; Operations</td>
</tr>
<tr>
<td>Staff</td>
<td>Director of Finance &amp; Operations</td>
</tr>
<tr>
<td>Student</td>
<td>Shared between the Registrar, Director of Admission</td>
</tr>
<tr>
<td>Alumnae</td>
<td>Development Officer</td>
</tr>
</tbody>
</table>

*The data steward may appoint a designee to serve in their place.
SSDS Technology staff serve as the data custodians for all data stored centrally on the school’s servers and administrative systems, and are responsible for the security of such data. For distributed data stored on departmental servers, the department head or their designee serves as the data custodian, and Technology Staff and the department share joint responsibility for securing the data.

Human Resources will inform Technology staff about an employee’s change of status or termination as soon as is practicable but before an employee’s departure date from the school. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee’s access to SSDS data.

Department heads will alert the Technology Staff at the conclusion of a contract for individuals that are not considered SSDS employees in order to terminate access to their SSDS accounts, if applicable.

The Technology Department is in charge of maintaining, updating, and implementing this Program. The School’s Technology Director has overall responsibility for this Program.

All members of the Community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the Community are required to access, store and maintain records containing sensitive data in compliance with this Program.

4.2 Identification and Assessment of Risks to school Information

The School recognizes that it has both internal and external risks to the privacy and integrity of school information. These risks include, but are not limited to:

- Unauthorized access of Confidential data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

The School recognizes that this may not be a complete list of the risks associated with the protection of confidential data. Since technology growth is not static, new risks are created regularly. Accordingly, the Technology Staff will actively participate and monitor for identification of new risks.
The School believes the school’s current safeguards are reasonable and, in light of current risk assessments made by Technology Staff, are sufficient to provide security and confidentiality to confidential data maintained by the school. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

4.3 Policies for Safeguarding Confidential Data

To protect school data classified as Confidential, the following policies and procedures have been developed that relate to access, storage, transportation and destruction of records.

Access & Storage

- Only those employees or authorized third parties requiring access to confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.
- To the extent possible, all electronic records containing Confidential data should only be stored on the school’s on-site secure network storage and not on local machines or unsecured servers.
- PHI may be stored or accessed through the Google Apps core suite (including Mail, Drive, Groups, Sites, Chat) as these apps are certified HIPAA compliant, provided that access to the PHI is appropriately restricted. This does not apply to Google consumer apps such as Google+, Hangouts, etc.
- Massachusetts PI and NFI must not be stored on any Google app.
- Confidential data must not be stored on cloud-based storage solutions that are unsupported by the school (including DropBox, Microsoft OneDrive, Apple iCloud, etc.).
- Members of the Community are strongly discouraged from storing Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport Confidential data electronically, the mobile device containing the data must be encrypted.
- Paper records containing Confidential data must be kept in locked files or other secured areas when not in use.
- Upon termination of employment or relationship with the School, electronic and physical access to documents, systems or other network resources containing Confidential data is immediately terminated.

Transporting Confidential Data

- Members of the Community are strongly discouraged from removing records containing Confidential data off site. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any unsecure location.
• When there is a legitimate need to provide records containing Confidential data to a third party outside the School, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

Destruction of Confidential Data

• Records containing Confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.

• Paper and electronic records containing Confidential data must be destroyed in a manner that prevents recovery of the data. Massachusetts General Law 93I specifies the manner in which records containing PI must be destroyed.

• In the event that transmission of student passport information is required by a hotel or program abroad in advance of the travel, only the relevant information requested (e.g., Name, Passport Number, Date of Expiry, and Date of Birth) will be provided, not complete copies of the passport images. This information should first be transmitted via fax or through eFax Secure website (SSL), provided that the School department arranging the travel confirms the accuracy of the fax number by sending an initial confirmation message before the actual data. If faxing is unavailable, the data may be sent via Schechter email, provided that the same confirmation of transmission takes place.

• Faculty/staff who need to retain these passport numbers for arranging travel will store this data in spreadsheets that are saved on the school’s secure server. Any spreadsheets containing student passport information should be routinely deleted by the spreadsheet owner when no longer needed.

• Faculty/staff who are traveling with the students abroad that need student passport and visa information for hotel check-in will keep a paper record on their person that contains relevant information (such as the passport and visa numbers and their expiry dates) and the last names of the students only. Faculty/staff must not retain or travel with copies of student passports.

• In extreme circumstances involving travel to a remote location where access to technology would be limited and would prohibit retrieval of a lost passport, a program director may request an exemption to this policy allowing for him or her to retain copies of the students passports during travel. This request will be made to the Chief Information Officer for approval. If the request is approved, the program director will acknowledge their understanding of the WISP and their responsibilities in protecting the passports. The program director also agrees to alert the School immediately if the copies of passport are lost.

4.4 Policies for Safeguarding Restricted Data

• Access to Restricted Data should be limited to members of the Community who have a legitimate business need for the data.

• Restricted Data can be stored on Google Apps and School secure servers.
● Restricted data may be stored on cloud-based storage solutions that are unsupported by the School as long as they comply with the requirements of any laws governing the protection of such data (e.g., FERPA).
● Documents containing Restricted Data should not be posted publicly.

4.5 Password Requirements

In order to protect SSDS data, all members of the Community must select unique passwords. SSDS maintains guidelines for password creation which include:

● Has at least 8 characters
● Contains a combination of at least three of the four character types: uppercase and lowercase letters, numbers, and special characters (e.g., @ $ # !)
● Does not contain words in any language, slang, dialect, jargon, etc., even if they are separated by numbers or special character (e.g., be87gin)
● Does not contain repeated characters or a sequence of keyboard letters (e.g., qwerty, 12345, or yyy99)
● Does not contain any part of the user’s name, username, birthday, or social security or those of friends and family (e.g., Jill1030)

Members of the community must protect the privacy of their passwords. Passwords must not be shared with others. If an account or password is suspected to have been compromised, all passwords should be changed immediately and the incident reported to the Technology Help Desk.

4.6 Third-Party Vendor Agreements Concerning Protection of Personal Information

The School exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the school to them. The primary budget holder for each department is responsible for identifying those third parties providing services to the school that have access to PI. All relevant contracts with these third parties are reviewed and approved by the School Business Office to ensure the contracts contain the necessary language regarding safeguarding PI. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect PI consistent with this Program and Massachusetts laws and regulations.

4.7 Computer System Safeguards

SSDS Technology Support Services staff monitor and assess safeguards on an ongoing basis to determine when enhancements are required. The school has implemented the following to combat external risk and secure the School network and systems containing Confidential Data:

● Secure user authentication protocols:
○ Unique passwords are required for all user accounts; each employee receives an individual user account.
○ Server accounts are locked after multiple unsuccessful password attempts.
○ Computer access passwords are disabled upon an employee’s termination.
○ **User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.**

- Secure access control measures:
  - Access to specific files or databases containing Confidential Data are limited to those employees who require such access in the normal course of their duties.
- SSDS Technology staff perform regular internal network security audits of all server and computer system logs as reasonable to discover to the extent of any possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of school data.
- Operating system patches and security updates are installed to all servers on a regular basis.
- Antivirus and anti-malware software is installed and kept updated on all workstations.

4.8 Employee Training

Following the adoption of this program, a copy of the WISP will be distributed to each employee who shall, upon receipt of the WISP, acknowledge in writing that he/she has received a copy of the document. All new employees will receive a copy of the WISP upon hire.

4.9 Reporting Attempted or Actual Breaches of Security - Incident Response Plan

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the CIO. The CIO will convene the Incident Team. The Chair is responsible for coordinating the Incident Team and determining appropriate actions in their response to the breach. The Incident Team will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Business Office. SSDS maintains a Cyber Risk Insurance policy, and the carrier will be notified immediately of any reportable incident.

5.0 Enforcement

Any employee or student who willfully accesses, discloses misuses, alters, destroys, or otherwise compromises Confidential or Restricted data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, up to and including termination in the case of employees and expulsion in the case of students.
6.0 Policies cross-referenced

The following SSDS policies provide advice and guidance that relates to this Program:

- Acceptable Use Policy (as written in the Employee Handbook)
- Password Guidelines

7.0 Effective date

This Written Information Security Program was implemented on xx/xx/xxxx, with revisions on xx/xx/xxxx.

The school will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to SSDS or the Community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure. Confidential data includes data that is protected by federal or state laws or regulations including the Health Insurance Portability and Accountability Act of 1996 (HIPAA)</td>
<td>• Social security numbers&lt;br&gt;• Credit/debit card number&lt;br&gt;• Financial account number&lt;br&gt;• Driver's license number&lt;br&gt;• Passport number&lt;br&gt;• Protected Health Information (PHI)</td>
</tr>
<tr>
<td>Restricted</td>
<td>Restricted data refers to all other personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations or reputation of Schechter Boston. It also includes data protected by the Family Educational Rights and Privacy Act (FERPA). This data should be limited to access by individuals who are employed by Schechter Boston and who have legitimate reasons for accessing such data, as governed by applicable law or school policy. Any non-public data that is not explicitly designated as Confidential should be treated as Restricted data.</td>
<td>• Student grades, transcripts etc.&lt;br&gt;• Donor information&lt;br&gt;• Information related to legal or Disciplinary matters.&lt;br&gt;• Student disciplinary, or judicial action information&lt;br&gt;• Police records&lt;br&gt;• School financial and investment records&lt;br&gt;• Employee salary information</td>
</tr>
<tr>
<td>Public (or unrestricted)</td>
<td>Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to SSDS or members of the SSDS community.</td>
<td>• Directory information&lt;br&gt;• All publicly available information</td>
</tr>
</tbody>
</table>
Schechter Boston Password Guidelines

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Schechter Boston’s entire network. As such, all Schechter employees (including contractors and vendors with access to Schechter systems) are asked to follow the password guidelines as outlined below, to select and secure their passwords.

General Password Construction Recommendations:

- Has at least 12 characters
- Has at least three of the four character types:
  - Uppercase letter
  - Lowercase letter
  - Number (0 – 9)
  - Special character. E.g. ? $ # ( )!
- Does not contain any part of your name, username, birthday, or social security or those of your friends and family. E.g. Jill1030

Password Management Guidelines

- Passwords should not be shared with others. In cases where password sharing is unavoidable, restricted accounts should be established to protect information resources.
- Passwords, if they need to be written down or stored on-line, must be stored in a secure place separate from the application or system that is being protected by the password. (i.e., no sticky-notes posted on the computer)
- Do not respond to email or phone requests to reveal username and password information.
- Do not use the “remember password” feature of applications unless the system or application has the means to encrypt the remembered password.
- Do not use Schechter passwords for non-Schechter sites (e.g., Facebook).
- Set browser defaults to clear password information each time the user exits the browser.
- Do not choose reset questions that may be easy for others to guess (e.g., Q: Name your favorite team: A: Red Sox).
- If an account or password is suspected to have been compromised, report the incident to the Technology Department immediately and change all passwords.
Schechter Boston Data Incident Response Plan

1.0 Policy Statement

The Solomon Schechter Day School ("SSDS" or the "School") Data Incident Response Plan outlines the School's actions following a data breach or other type of data related incident in order to ensure timeliness of response, compliance with applicable laws and regulations and ensure consistency in all aspects of the School's response.

2.0 Background

The number of data breaches worldwide increases every year, as a result of hackers attempting to capture confidential and/or protected information. Academic institutions are at risk because of the kinds of sensitive information they maintain. Data breaches can occur anywhere that information resides, including computer systems, portable media, paper records, etc.

SSDS is committed to protecting the privacy of its community, which includes safeguarding the sensitive and protected data that is owned and maintained by the school. Schechter Boston has taken many steps to reduce the risk of breach of such data, many of which are outlined in the School's Written Information Security Program (WISP).

However, no protection is foolproof, and many data breaches occur as a result of human error. Therefore, the School must be prepared to respond to a breach in the event that one should occur.

3.0 Purpose

In accordance with federal and state laws and regulations, SSDS is required to provide notice about security breaches of protected information at the school to affected individuals and appropriate state agencies. SSDS is also committed to protecting other kinds of sensitive institutional information that is maintained at the School. In the event that sensitive and/or protected information at the School is exposed as a result of a breach, the School will take steps to:

- Prevent further exposure,
- Contact the Cyber Security Liability insurance carrier
- Investigate the incident and support law enforcement if criminal activity is suspected,
- Determine any legal obligations,
- Notify the departments and individuals affected,
- Respond to media inquiries,
- Document any responsive actions taken, and
- Conduct a post-incident review of these actions.

Accomplishing the above tasks will necessarily involve individuals from diverse areas within and outside of the School and will require that a plan be in place to address a breach before it occurs. The purpose of this plan is to outline the School’s response to a data breach, including procedures for reporting a breach and individual team members’ responsibilities following a breach.
4.0 Scope

The Incident Response Plan addresses four types of information compromises:

1. Computing Devices Compromised by Malware
2. Computing Devices Compromised by Unauthorized Access (includes any devices accessed without permission, either by stolen or compromised credentials, or other attempts to access a device without authorization)
3. Lost or Stolen Computing Devices
4. Lost or Stolen Paper Records containing Confidential Data, as defined below

The scope includes all computing devices (both School-owned and personal), including computers, servers, portable media, external hard drives or other mobile devices, and all paper records, which contain confidential data. All Schechter Boston employees that maintain or access confidential data, both paper and electronic, at the school must comply with this plan.

4.1 Definitions

**Breach of security**: The unauthorized acquisition or use of sensitive or protected data that creates a substantial risk of identity theft, fraud or harm to the reputation or business interests of an individual or institution.

**Compromised computer**: Identifying an impacted device can be difficult. Some ways a compromised computer can be identified include: the computer user suspects that his/her system is exhibiting suspicious behavior or has suspicious files stored on the device; network or system logs indicate unusual network behavior coming from or going to the device; or individuals at the School or outside of the School report cyber-attacks or unusual network behavior emanating from the device.

**Confidential data**: Refers to any information, both paper and electronic, that is protected by Federal, state, or local laws and regulations, or other sensitive personal and institutional data where the loss of such data could harm an individual’s right to privacy or negatively impact the finances, operations or reputation of the School. Protected data includes Personal Information (defined below), student education records, and Protected Health Information (PHI). For a more complete description of these terms and the types of data identified as Confidential, see the School’s Written Information Security Program (WISP).

**Personal Information**: Personal Information (PI), as defined by Massachusetts law (201CMR17.00), is the first name and last name, or first initial and last name of a person in combination with any one or more of the following: 1) Social Security number; 2) Driver’s license number or state-issued identification card number; or 3) Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person’s financial account, with or without any required security code, access code, personal identification number, or password. As defined by the WISP, PI also includes passport number, alien registration number or other government-issued identification number.

**SSDS Employees**: Includes all Schechter employees, whether full- or part-time, including faculty, administrative staff, contract and temporary workers, hired consultants, interns, and student employees.

5.0 Responsibilities

The School’s Technology department is charged with the identification of all data security incidents involving electronic data or paper records where the loss, theft, unauthorized access, or other exposure of confidential data is suspected. When the technology department confirms an incident involving confidential electronic data,
they will alert the Director of Finance & Operations. The Director of Finance & Operations will determine appropriate actions in their response to the breach.

The Director of Finance & Operations will oversee the investigation of the incident and involve legal counsel, insurance carrier, and local, state, and federal law enforcement as necessary. The severity of the breach will determine the nature of the investigation, including what authorities are involved and how evidence is collected.

The technology department will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Business Office.

All SSDS employees are responsible for identifying and reporting potential security breaches. For help with security issues, including descriptions of the various types of security breaches and how to report them, see the technology department for guidance.

6.0 Response Plan

For suspected data breaches, the Technology Department will:

- Conduct a preliminary investigation: Gather details about the incident, including when the breach was first discovered and how the employee responded. In cases involving electronic data, they will also inquire about symptoms of the compromised computing device.
- Determine if confidential data was involved: Inquire about the nature of records or data involved in the breach and what kinds of information it contained. For electronic data breaches, the Technology Department will use a variety of technologies to determine if confidential data was present on the compromised device. If the computing device was stolen, the technology department will do the analysis on backups. If backups are not available, the severity of the incident will be classified based on the individual's access to various sensitive data.

If an incident involving confidential data is confirmed, the Technology Department will contact the Director of Finance & Operations. The Director will:

- Notify Senior Staff: Provide details about the incident and provide status updates.
- Convene the Incident Team: If PI, PHI or student education records were determined to be involved in the data breach, or if the presence of sensitive data could not be ruled out, the Director will convene the Incident Team.
- Consult Legal Counsel: The Director and Incident Response Team will consult the School’s legal counsel to review the incident to determine the School’s legal obligations for reporting under applicable federal and state laws.
- Notify the Cyber Security Liability Insurance Carrier of potential claim and generate a claim number as necessary.
- Notify affected individuals: Under Massachusetts General Law Chapter 93H, and The Health Information Technology for Economic and Clinical Health (HITECH) Act, the School is required to notify any individuals whose personal information or protected health information (respectively) may have been compromised as a result of this incident (regardless of confirmation of identity theft). Depending on the circumstances of the breach, the School may be obligated to notify other individuals and agencies as prescribed as law. The nature of the breach will also determine the method(s) of notification.

7.0 Enforcement
Any employee who neglects to report a known security breach, or who fails to comply with this plan in any other respect, will be subject to disciplinary action.

8.0 Policies Cross-Referenced

FERPA Policy
HIPAA Privacy Notice
Written Information Security Program

9.0 Effective Date

This plan was implemented on 11/1/202.

The school will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.