

**STANDARD STUDENT DATA PRIVACY AGREEMENT**

**MASSACHUSETTS, MAINE, NEW HAMPSHIRE, NEW YORK, RHODE ISLAND AND VERMONT**

**MA-ME-NH-NY-RI-VT-NDPA, Standard Version 1.0**

**Broome-Tioga Board of Cooperative Educational Services (BOCES)**

**and**

**FrontEdge Inc.**

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between: Broome-Tioga BOCES, located at 435 Glenwood Rd Binghamton, NY 13905-1699 (the “Local Education Agency” or “LEA”) and FrontEdge Inc., located at 274 Goodman Street North, Rochester, NY, 14607 (the “Provider”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
  - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “Services”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Adam Rene Title: Director, Information Technology  
Address: 274 N Goodman St Suite 265, Rochester, NY 14607  
Phone: 1 585-532-7747  
Email: adam@schoolfront.com

The designated representative for the LEA for this DPA is:

Ashleen Speen, Associate Coordinator of Data Security & Privacy  
4937 Spring Rd Vernoia, NY 13478  
607-427-4423  
aspeen@btbooces.org

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**Broome-Tioga BOCES**

By: *Christine Choi*  
Date: 3/1/2024

Printed Name: Christine Choi  
Title/Position: Executive Operations Officer

FrontEdge Inc. *Adam Rene*  
By: \_\_\_\_\_  
Date: 12/11/2023

Printed Name: Adam Rene  
Title/Position: Director, Information Technology

## **STANDARD CLAUSES**

Version 1.0

### **ARTICLE I: PURPOSE AND SCOPE**

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- 2. Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
- 3. DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

### **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

- 1. Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
- 2. Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
- 3. Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
- 4. Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2)

research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after six (6) months. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

## **ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security

programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
  - i. The name and contact information of the reporting LEA subject to this section.
  - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
  - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
  - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

#### **ARTICLE VI: GENERAL OFFER OF TERMS**

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

- 1. Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
- 2. Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
- 3. Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
- 4. Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
- 5. Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
- 6. Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
- 7. Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.



8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
  
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

## EXHIBIT "A"

### DESCRIPTION OF SERVICES

**SchoolFront**, a highly-secure, customizable web-based K-12 school district management platform. A modular array of software features designed to optimize school district administrative operations under a single integrated platform.

Note: The applicability of data categories does vary based on whether a contracting LEA has purchased and is using certain modules. For example, Exhibit B, the schedule of data for student data is not applicable to LEAs who do not use SchoolFront's Student Information System (SIS) modules.

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

<b>Category of Data</b>	<b>Elements</b>	<b>Check if Used by Your System</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify:	Browser, OS version, screen resolution, page accesses
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	X
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	X
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X

Category of Data	Elements	Check if Used by Your System
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	X
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data -Please specify:	
Transcript	Student course grades	X
	Student course data	X
	Student course grades/ performance scores	X
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	

Category of Data	Elements	Check if Used by Your System
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

## EXHIBIT "C" DEFINITIONS

**De-Identified Data and De-Identification:** Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**Operator:** means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

**Student Generated Content:** The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal

records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

**Subprocessor:** For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

**[Insert Name of District or LEA]** Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

\_\_\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

**[Insert categories of data here]**

\_\_\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions]**

3. Schedule of Disposition

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By **[Insert Date]**

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date



**EXHIBIT “F”**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**  
**2/24/2020**

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* (“Cybersecurity Frameworks”) that may be utilized by Provider .

Cybersecurity Frameworks

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input checked="" type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input checked="" type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**EXHIBIT "G"**  
**Massachusetts**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

## **EXHIBIT "G"**

### **Maine**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
  - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
  - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
  - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

**EXHIBIT "G"**  
**Rhode Island**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
    1. The credit reporting agencies
    2. Remediation service providers
    3. The attorney general
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
  - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

## **EXHIBIT "G"**

### **Vermont**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

**EXHIBIT "G"**  
**New Hampshire**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.  
Date of birth.  
Personal street address.  
Personal email address.  
Personal telephone number  
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "1"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
- (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - (2) Limit unsuccessful logon attempts;
  - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
  - (4) Authorize wireless access prior to allowing such connections;
  - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
  - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
  - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
  - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
  - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
  - (10) Perform maintenance on organizational systems;
  - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
  - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
  - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
  - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
  - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
  - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.



**EXHIBIT "I" – TEACHER DATA**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	Browser, OS version, screen resolution
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries)	X
Demographics	Date of Birth	X
	Place of Birth	
	Social Security Number	X
	Ethnicity or race	X
	Other demographic information-Please specify:	Gender
Personal Contact Information	Personal Address	X
	Personal Email	X
	Personal Phone	X
Performance evaluations	Performance Evaluation Information	X
Schedule	Teacher scheduled courses	X
	Teacher calendar	X
Special Information	Medical alerts	
	Teacher disability information	ADA accomodations
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Teacher app username	X
	Teacher app passwords	X
Teacher In App Performance	Program/application performance	X
Teacher Survey Responses	Teacher responses to surveys or questionnaires	X
Teacher work	Teacher generated content; writing, pictures etc.	X
	Other teacher work data -Please specify:	Personnel file contents
Education	Course grades from schooling	X
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

## **Exhibit "G"**

### **New York**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

**WHEREAS**, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
7. To amend Article II, Section 6 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA’s Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor’s Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.
8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **“Exhibit D”**.

11. To amend Article IV, Section 7 to add: ‘Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, “which term shall not include students.”
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department’s Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Contractor to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider’s expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider’s privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the

incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident.

Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
  - i. The name and contact information of the reporting LEA subject to this section.
  - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
  - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
  - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
  - vi. The number of records affected, if known; and
  - vii. A description of the investigation undertaken so far; and
  - viii. The name of a point of contact for Provider.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.
-

**Exhibit “J”**  
**LEA Documents**

LEA’s Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement can be accessed at:

[https://drive.google.com/file/d/1kN6Q9wRUvfpVgDEL\\_g9LSRdW7\\_UeEZ6H/view?usp=sharing](https://drive.google.com/file/d/1kN6Q9wRUvfpVgDEL_g9LSRdW7_UeEZ6H/view?usp=sharing)

**Exhibit "K"**  
**Provider Security Policy**

Provider's Data Security and Privacy Plan can be accessed at:

See Attached "SchoolFront Information Security Policy.pdf"

---






# SchoolFront\_Broome-TiogaBOCES\_VendorSigned

Final Audit Report

2024-03-01

Created:	2024-03-01
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAASXH_QI80hAKc26rsIx7DHMFwP0GJvYY1

## "SchoolFront\_Broome-TiogaBOCES\_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2024-03-01 - 12:12:15 PM GMT - IP address: 108.35.203.7
-  Document emailed to Christine Choi (cchoi@btboces.org) for signature  
2024-03-01 - 12:13:15 PM GMT
-  Email viewed by Christine Choi (cchoi@btboces.org)  
2024-03-01 - 12:24:19 PM GMT - IP address: 74.67.107.59
-  Document e-signed by Christine Choi (cchoi@btboces.org)  
Signature Date: 2024-03-01 - 12:25:18 PM GMT - Time Source: server- IP address: 74.67.107.59
-  Agreement completed.  
2024-03-01 - 12:25:18 PM GMT

## SchoolFront

[www.schoolfront.com](http://www.schoolfront.com)

274 N. Goodman St. Suite B265

Rochester, New York 14607

[www.frontedge.com](http://www.frontedge.com)



SchoolFront

# SchoolFront

## *Company Information Security Policy (ISP)*

### Policy Revision / Update

Date	By
02/28/2020	Thomas Karafonda
03/18/2021	Casey Karafonda
03/28/2022	Thomas Karafonda

---

sales

588.568.7813

[sales@schoolfront.com](mailto:sales@schoolfront.com)

support

585.568.7813

[support@schoolfront.com](mailto:support@schoolfront.com)

<https://support.schoolfront.com>



## Table of Contents

Introduction .....	4
Roles and Information Security Responsibility .....	5
Information Security Officer .....	5
Information Technology Administrator .....	5
Company Asset Users.....	6
Third-Party Company Asset Users .....	6
NYS BOCES .....	7
BOCES Customers and NYS Education Law § 2-d.....	8
BOCES Customers and HIPAA .....	8
BOCES Customers and Social Security Number Protection .....	9
Customers.....	9
Customers and NYS Education Law § 2-d .....	10
Customers and HIPAA.....	10
Customers and Social Security Number Protection.....	10
RecruitFront Job Applicants.....	10
Colleges and Universities (Registrar) .....	11
Additional Roles and Responsibilities When Handling PI.....	12
NYS Education Law § 2-d.....	12
Customer Responsibilities as an Educational Institution .....	12
Company Responsibilities as a Third-Party Contractor .....	13
HIPAA.....	14
Customer Responsibilities as a HIPAA Covered-Entity .....	14
Company Responsibilities as a Business Associate of a Covered-Entity .....	15
NYS Social Security Number Protection .....	15
Customer Responsibility Under NYS SS# Protection Law .....	16
Company Responsibility Under NYS SS# Protection Law.....	16
Information Security Procedures and Guidelines .....	17
Administrative Safeguards.....	17
Assigned Security Responsibility .....	17
Risk Analysis .....	17
Risk Management.....	17
Violations / Sanctions .....	17



Acceptable Use .....	18
Information System Activity Review .....	21
Workforce Security .....	21
Information Access Management.....	23
Security Communication, Awareness, and Training.....	24
Password Management .....	25
Security Incident Procedures & Reporting.....	26
Incident Response Plan.....	27
Routine Monitoring and ISP Compliance Evaluations.....	29
Physical Safeguards.....	31
Environmental Access Controls and High-Availability.....	31
Workstation and Mobile Device Use .....	34
Device and Media Controls.....	41
Technical Safeguards.....	42
Access Control .....	42
Audit Controls .....	43
Integrity .....	44
Person or Entity Authentication and Authorization .....	45
Transmission Security .....	45



## Introduction

The purpose of this **Information Security Policy ("ISP")** is to provide a security and privacy framework that will:

1. Ensure the protection, confidentiality, integrity, acceptable use, and availability of SchoolFront (“**Company**”) information assets, physical assets, Company information, and customer information (collectively, “**Company Assets**”).
2. Ensure the protection, confidentiality, integrity, acceptable use, and availability of Customers of the Company (“**Customer**”) information assets, physical assets, and Customer information (collectively, “**Customer Assets**”).
3. Ensure the protection, confidentiality, integrity, acceptable use, and availability of legally **Protected Information (PI)** accessible by any [Company Asset Users](#) and/or [Third-Party Company Asset Users](#).
4. Comply with PI-related legislation, regulations, and best practices and protect the Company, the Company’s employees, the Company’s customers, and the people served by the Company’s customers.

The development and ongoing maintenance of this ISP is informed by the output of routine Company [Risk Analysis](#), and includes the following elements:

1. Information security policies and procedures to provide for the confidentiality, integrity, and availability of Company Assets, Customer Assets, and PI;
2. Annual risk analysis to identify and assess reasonably foreseeable risks based on present threats and vulnerabilities to the security and confidentiality of Company Assets, Customer Assets, and PI;
3. Security Awareness Training and Education, which emphasizes the importance of protecting Company Sensitive Information and personally identifiable information during different states, as well as how and when to report a potential security breach or incident to Information Security;
4. Investigation of improper behavior or potential criminal acts generated or transmitted electronically utilizing qualified personnel with investigative training, experience, and knowledge in pertinent laws and toolkits for doing forensics;
5. Monitoring and auditing of all aspects of the Company’s use and implementation of, and compliance with, the ISP;
6. Monitoring for intrusions or other unauthorized use;
7. Annually revisiting information security policies and procedures for changes in laws, as well as technology and standards change;
8. Support for Company Human Resources personnel with ensuring continuity between the ISP and its operating procedures, such as background investigations, terminations, computer breaches, fraud, embezzlement, unlawful acts or other forms of dishonesty and violations of Company policies; and



9. An Incident Response Plan that includes breach notification procedures.

## Roles and Information Security Responsibility

### Information Security Officer

The Information Security Officer (ISO) is responsible for:

- Conducting and communicating the output of continuous Company Risk Assessment.
- Establishing required minimum-security standards for handling Company Assets, Customer Assets, and PI—the ISP.
- Monitoring and reviewing the implementation and day-to-day adherence to the ISP.
- Performing and retaining the results of appropriate human resources vetting activities for new Company hires.
- Managing an information security training and awareness program for all employees of the Company.
- Overseeing security for Company networks and systems, and any systems connecting to the Company.
- Handling information security incidents, and incident reporting for the Company.
- Updating the ISP as appropriate in response to the findings of Continuous Company Risk Assessment.
- Updating the ISP as appropriate to maintain compliance with changing legal regulations, technical advancements, and improved industry best practices.
- Managing all Company security and privacy-related communication both internally and externally.
- Facilitating security and privacy-related audits as legally required.

### Information Technology Administrator

The **Information Technology Administrator (ITA)** may or may not supervise a team, the **Information Technology Team (IT Team)**, to support his/her responsibilities. The ITA (with support of the IT Team, if applicable) is responsible for:

- Ensuring that all standards and practices detailed in the ISP are implemented in the deployment and use of the Company network, as well as followed by Company and Third-Party Company Asset Users provided electronic access to Company Assets, Customer Assets, and/or PI.
- Administrating information systems and networks in a manner that protects the confidentiality, integrity, and availability of Company Assets, Customer Assets, and PI



that is stored in them or transmitted through them, including all systems that are connected to internal networks, consistent with the Company's ISP.

- Authorizing Company employees to access Company Assets, Customer Assets, and/or PI.
- Authorizing and de-authorizing Company employee access to Company information/data, services, and other resources based on the principle of least privilege, and in a manner that supports individual accountability for user activity.
- Obtaining and maintaining authorization for access to and use of federal- and/or state-regulated PI.

## Company Asset Users

**Company Asset Users** are Company employees who have been authorized by the ITA to access Company Assets. Company Asset Users are responsible for:

- Understanding and adhering to Company policies.
- Complying with best practices in information security as established by the ISO and communicated via the ISP.
- Reporting suspected or known compromises of Company Assets, Customer Assets, and PI, immediately upon discovering the known or suspected compromise, as described in the [Procedures for Reporting a Security Incident](#).
- Securely managing all Company Assets, Customer Assets, and PI in their possession, including information for which the user is not the originator but a subsequent recipient, as well as information originated by the user but intended for use by others.
- In addition to the directives specified by law and in the Company ISP, these individuals are expected to exercise good judgment in maintaining the security of all Company Assets, Customer Assets, and PI.

## Third-Party Company Asset Users

Security and Privacy terms are a required component of all agreements entered into by the Company which grant a third-party access to Company Assets, Customer Assets, and/or PI. All such agreements should be reviewed and approved by the ISO prior to signing to ensure that Company ISP compliance is stipulated.

**Third-Party Company Asset Users** are people or organizations that are not a component or employees of the Company, who have been authorized by the ISO following acknowledgement and acceptance of a formal agreement detailing their specified level of access to Company Assets, Customer Assets, and/or PI AND acknowledgement and formal acceptance (e.g. via signature) of the Company ISP.



Third-Party Company Asset Users have the same responsibilities as Company Asset Users, with the additional responsibility of adhering to the terms of their formal third-party agreement(s) with the Company.

## NYS BOCES

New York State Boards of Cooperative Educational Services (BOCES) provide shared educational programs and services to school districts within the state. There are approximately 37 BOCES that partner with nearly all of the state's school districts to help meet students' evolving educational needs through cost-effective and relevant programs. Under Education Law section 1950, a BOCES may provide any educational service that is requested by two or more component districts and approved by the commissioner of education according to need and practicality in a regional context.

The Company has established cooperative agreements with BOCES throughout NYS via formal "CO-SER" agreements wherein the BOCES provisions Company Services (e.g. SchoolFront, RecruitFront, Scanning, etc.) on behalf of the Company for two or more NYS school districts. These formal agreements with BOCES organizations include terms to explicitly protect Company Assets, school district Assets (protected by CO-SER agreements), and PI, and detail both Company and BOCES responsibility in the ongoing maintenance of Company Asset, BOCES Asset, Customer Asset, and PI security.

The Company abides by BOCES and CO-SER school district security and privacy requirements enforced by these formal BOCES CO-SER Agreements and ensures that Third-Party Company Asset Users are educated on and compliant with the terms of these agreements.

See [Third-Party Agreements and Access to Company Assets, Customers Assets, and PI](#).

**NYS BOCES End-Users ("BOCES Users")** are people or organizations granted access to BOCES information assets, physical assets, and CO-SER school district assets to which the BOCES is authorized access by formal BOCES CO-SER agreements between the BOCES and a school district (collectively "**BOCES Assets**") by the BOCES. BOCES Users may access the BOCES Assets and PI via Company Services like SchoolFront and/or RecruitFront ("Company Services"). The level of access they enjoy is controlled in full by the BOCES. BOCES Users are responsible for adhering to the rules and requirements of the BOCES who granted them access.

BOCES Assets (e.g. data, etc.) housed/managed in Company Services (e.g. SchoolFront, RecruitFront) are partitioned and secured so that BOCES cannot access specific school district assets without authorization. Within a BOCES's partition, BOCES Assets are further secured by system roles (with varying degrees of BOCES Asset access and permissions) which may be assigned to or revoked from BOCES Users by BOCES Administrators.

**BOCES Administrators** are BOCES Users with broad access (granted by the BOCES) to BOCES Assets within Company Services, who manage systems and services on behalf of the BOCES or otherwise have elevated privileges. Some BOCES Administrators have the ability to authorize/assign access to other BOCES Users. The decision to assign such elevated privileges and access to Company Services and the BOCES Assets and PI within them is at the sole discretion of the BOCES.





BOCES are responsible for the following security-related functions:

- Providing and supporting the tools and services required to securely connect BOCES Users to Company Services.
- Mitigating the privacy and security risks associated with granting BOCES Users access to BOCES Assets and PI by upholding school district CO-SER agreements and communicating and enforcing their own BOCES requirements for privacy and security among BOCES Users.
- Monitoring / reviewing BOCES User activity in Company Systems used by the BOCES to identify risky BOCES User behavior and violations of BOCES, CO-SER school district, and state and federal security and privacy rules.
- All BOCES User authorization and management including granting and revoking Company Services access to BOCES Users.
- Managing BOCES Assets (e.g. BOCES Data and BOCES CO-SER school district Data, etc.).
- Authorizing the Company to access BOCES CO-SER school district Assets so that the Company may perform/support BOCES CO-SER services.
- Initiating and facilitating the engagement between the Company and third-party organizations with whom the BOCES desires the Company to partner / integrate and authorizing the agreements between the Company and such third-party organizations.
- Reporting suspected or confirmed security/privacy violations that involve or impact the Company.  
See [Incident Reporting](#).
- Participating in incident response activities in the event of an incident impacting the BOCES and/or its CO-SER school districts.  
See [Incident Response Plan](#).

## BOCES Customers and NYS Education Law § 2-d

When the Company contracts with a BOCES to perform services or CO-SER, the Company is generally governed as a “third-party contractor” under NYS Education Law § 2-d.

See [NYS Education Law § 2-d](#).

## BOCES Customers and HIPAA

When the Company contracts with a BOCES to perform services or CO-SER *and* the BOCES meets the criteria for a “covered entity” under the Health Insurance Portability and Accountability Act (HIPAA), the Company is generally governed as a “business associate.”

See [HIPAA](#).



## BOCES Customers and Social Security Number Protection

The Company's BOCES Customers sometimes request and store, for various legally-allowed purposes, BOCES End-User (employee) social security numbers, PI the care and handling of which requires special consideration under NYS law.

See [NYS Social Security Number Protection Law](#).

## Customers

**Customers** are people or organizations who have purchased services from the Company under the terms of a formal agreement. All formal Company Customer agreements include terms to explicitly protect Customer Assets and PI, and detail both Company and Customer responsibility in the ongoing maintenance of Customer Asset and PI security.

The Company abides by Customer security and privacy requirements enforced by formal Customer Agreements and ensures that Third-Party Company Asset Users are educated on and compliant with the terms of Company Customer Agreements.

See [Third-Party Agreements and Access to Company Assets, Customers Assets, and PI](#).

**Customer End-Users ("End-Users")** are people or organizations granted access to Customer Assets *by the Customer*. Customer End-Users may access Customer Assets and PI to which they have Customer-authorized access via Company Services such as, SchoolFront and/or RecruitFront ("**Company Services**"). The level of access they enjoy is controlled in full by the Customer. Customer End-Users are responsible for adhering to the rules and requirements of the Customer who granted them access.

Customer Assets (e.g. data, etc.) housed/managed in Company Services (e.g. SchoolFront, RecruitFront) are partitioned and secured so that Customers cannot access other Customer Assets without authorization. Within a Customer's partition, Customer Assets are further secured by system roles (with varying degrees of Customer Asset access and permissions) which may be assigned to or revoked from End-Users by Customer Administrators.

**Customer Administrators** are End-Users with broad access (granted by the Customer) to Customer Assets within Company Services, who manage systems and services on behalf of the Customer or otherwise have elevated privileges. Some Customer Administrators have the ability to authorize/assign access to other Customer End-Users. The decision to assign such elevated privileges and access to Company Services and the Customer Assets and PI within them is at the sole discretion of the Customer.

Customers are responsible for the following security-related functions:

- Providing and supporting the tools, services, and policy necessary to securely connect their End-Users to Company Services.
- Mitigating the privacy and security risks associated with granting their End-Users access to their Customer Assets and PI by communicating and enforcing their own organizational requirements for privacy and security among End-Users.



- Monitoring / reviewing End-User activity in Company Systems used by the Customer to identify risky End-User behavior and violations of Customer security and privacy rules.
- All End-User authorization and management including granting and revoking Company Services access to End-Users.
- Managing Customer Assets (e.g. Customer Data, etc.).
- Authorizing the Company to access Customer Assets in order to perform services for the Customer.
- Initiating and facilitating the engagement between the Company and third-party organizations with whom the Customer desires the Company to partner / integrate and authorizing the agreements between the Company and such third-party organizations.
- Reporting suspected or confirmed security/privacy violations that involve or impact the Company.  
See [Incident Reporting](#).
- Participating in incident response activities in the event of an incident impacting the Customer.  
See [Incident Response Plan](#).

## Customers and NYS Education Law § 2-d

When the Company contracts with a Customer to perform services, the Company is generally governed as a “third-party contractor” under NYS Education Law § 2-d.

See [NYS Education Law § 2-d](#).

## Customers and HIPAA

When the Company contracts with a Customer to perform services *and* the Customer meets the criteria for a “covered entity” under the Health Insurance Portability and Accountability Act (HIPAA), the Company is generally governed as a “business associate.”

See [HIPAA](#).

## Customers and Social Security Number Protection

The Company’s Customers sometimes request and store, for various legally-allowed purposes, Customer End-User social security numbers, PI the care and handling of which requires special consideration under NYS law.

See [NYS Social Security Number Protection Law](#).

## RecruitFront Job Applicants

**RecruitFront Job Applicants** are people who browse, register on, use for job applications, or otherwise access the Company’s service, RecruitFront, including without limitation:



- RecruitFront.com,
- Support.RecruitFront.com,
- App.RecruitFront.com, and
- X.recruitfront.com where “X” is a name defined by a FrontEdge Client.

RecruitFront Job applicants are governed and protected by the [RecruitFront Terms of Use](#), which they formally agree to by accessing RecruitFront in any capacity.

## Colleges and Universities (Registrar)

The Registrar of colleges and universities (“**University Registrars**”) are invited to securely upload official transcripts for students applying for employment opportunities in electronic format in SchoolFront.

University Registrars who use this methodology are responsible for:

- Working with the appropriate [NYS BOCES](#) organization to gain SchoolFront electronic transcript upload access.
- Providing and supporting the tools and services required to securely connect University Registrar Staff (“**Registrar Staff**”) to SchoolFront.
- Providing and supporting the process(es), tools, and services required to verify the authenticity of electronic transcripts uploaded to SchoolFront by Registrar Staff.
- Mitigating the privacy and security risks associated with granting Registrar Staff access to SchoolFront by communicating and enforcing their own organizational requirements for privacy and security.
- Monitoring electronic transcript upload transactions in SchoolFront to ensure their own organizational requirements are being followed.
- Submitting formal requests for Registrar User account changes (including new accounts and closed accounts) to the SchoolFront Support Team for processing via the Support Portal. <https://support.schoolfront.com/> or <https://support.recruitfront.com/>.
- Reporting suspected or confirmed security/privacy violations that involve or impact the Company.  
See [Incident Reporting](#).
- Participating in incident response activities in the event of an incident impacting the Customer.  
See [Incident Response Plan](#).



## Additional Roles and Responsibilities When Handling PI

### NYS Education Law § 2-d

Many of the Company's Customers, including BOCES, are educational agencies for whom the Company is considered a third-party contractor under [New York State Education Law § 2-d](#).

In addition to standard security and privacy related roles and responsibilities, the Customer and Company have additional responsibilities under NYS Education Law § 2-d.

### Customer Responsibilities as an Educational Institution

When a Customer is an Educational agency subject to the terms of NYS Education Law § 2-d and the Company requires access to Customer information that is protected under NYS Education Law § 2-d to perform contracted services, unless otherwise specified in a formal agreement between the Customer and the Company, the Customer is responsible for:

- Creating and publishing a Parent's Bill of Rights for Data Privacy and Security on their website.
- Publishing supplemental Third-Party Contractor (Company) compliance information as required/necessary with their Parent's Bill of Rights for Data Privacy and Security.
- Ensuring that the terms of their Parent's Bill of Rights for Data Privacy and Security are acknowledged in Company Services agreement(s).
- Creating and managing compliant procedures related to all types of requests related to access to Customer PI (i.e. Student and Teacher/Principal PII, etc.) and challenges to the accuracy of Customer PI accessible via Company Services.
- Reporting every discovery, report of a breach, or unauthorized release of data to the Customer's Chief Privacy Officer, in the timeframe and format required by the New York State Education Department.
- Reporting any breach or unauthorized release of PI to law enforcement if the incident is believed to constitute criminal conduct.
- Notifying parents, eligible students, teachers and/or principals affected by a breach or unauthorized release of data per the guidelines for breach notification set forth in NYS Education Law § 2-d.
- Cooperating with law enforcement to protect the integrity of investigations regarding breach or unauthorized release of PI.
- Securely retaining Customer assets including PI, as required, following the conclusion of the formal Customer Agreement with the Company.



## Company Responsibilities as a Third-Party Contractor

When a Company Customer is an Educational agency subject to the terms of NYS Education Law § 2-d and the Company requires access to Customer information that is protected under NYS Education Law § 2-d to perform contracted services, unless otherwise specified in a formal agreement between the Customer and the Company, the Company is responsible for:

- Managing the access of Company and Third-Party Company Asset users to Customer Assets and PI, including:
  - Thoroughly vetting Company and Third-Party Company Asset users before authorizing their access to Customer Assets and PI.
  - Providing training to Company and Third-Party Company Asset users on the state and federal laws and regulations governing PI prior to granting access to Customer Assets and PI.  
See [Security Awareness, Communication, and Training](#).
  - Ensuring Company and Third-Party Company Asset users are allowed only the minimal access to Customer Assets and PI that they need to do their job.
  - Ensuring that Company and Third-Party Company Asset User Customer Asset and PI access levels are reviewed and adjusted as necessary when their role for the Company changes, including upon employment / third-party contract conclusion/termination.  
See [Workforce Security](#).
- Monitoring Company and Third-Party Company Asset users with access to Customer Assets and PI to ensure that they adhere to Company [Acceptable Use](#) rules and access/use PI exclusively for the purposes defined in Customer agreements.  
See [Routine Monitoring and ISP Compliance Evaluations](#).
- Leveraging technologies, practices, and safeguards that align with the NIST CSF and comply with Customer data security and privacy policy, including:
  - Using encryption technology to protect data while in motion and in Company custody from unauthorized disclosure using controls as specified by the Secretary of HHS in guidance issued under Public Law 111-5, § 13402(h)(2).
  - Securely retaining and backing-up Customer Assets housed in Company Services.  
See [Data Back-up](#) and [Data Retention](#).
  - Securely housing Company Services and Customer Assets and PI in environments that reflect industry best-practices and comply with state and federal laws and regulations for privacy and security.  
See [Physical Safeguards](#).
  - Implementing and monitoring the compliance of the Company ISP, including [Administrative Safeguards](#), [Physical Safeguards](#), and [Technical Safeguards](#).



- Providing Company and Third-Party Company Asset Users with training and guidelines for the secure handling of Company and Customer Assets and PI at all times.  
See [Security Awareness, Communication, and Training](#).
- Returning and/or destroying, as applicable, Customer Assets and PI in Company possession following the conclusion/termination of the Customer agreement, per the terms of the agreement.  
See [Data Back-up](#) and [Data Retention](#).
- Directing all requests for access to, or challenges to the accuracy of, Customer Assets and PI (i.e. by parents, guardians, students, teachers, or any other type of Customer End-User) to the Customer for handling.
- Reviewing and accepting Customers' Parent's Bill of Rights for Data Privacy and Security.
- Forbidding and protecting against the sale, use, or disclosure of Customer PI by the Company or Third-Parties for marketing or commercial purposes.
- Performing [routine risk assessment](#) and updating the Company ISP and ISP implementation as necessary to mitigate new/changed risk.
- Monitoring Company and Third-Party compliance with the Company ISP.
- Promptly notifying impacted Customer(s) of any breach or unauthorized release of Customer PI no later than seven (7) calendar days after discovery of a breach.  
See [Incident Response Plan - Breach Notification](#).
- Cooperating with the Customer and law enforcement to protect the integrity of investigations regarding breach or unauthorized release of PI.

## HIPAA

HIPAA Covered Entities are Customer organizations for whom the Company is typically considered a “business associate” under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) if the Customer is responsible for the management of PI as defined under HIPAA.

In addition to standard security and privacy related roles and responsibilities, the Customer and Company have additional responsibilities under HIPAA.

### Customer Responsibilities as a HIPAA Covered-Entity

When a Customer is a HIPAA covered-entity and the Company requires access to HIPAA PI to perform contracted services, unless otherwise specified in a formal agreement between the Customer and the Company, the Customer is responsible for:

- Complying with HIPAA requirements for Covered Entities.



- Ensuring that the contract/agreement signed between the Customer and Company meets the requirements for Business Associate contracts with a covered entity under HIPAA.
- Securely retaining Customer assets including PI, as required, following the conclusion of the formal Customer Agreement with the Company.

## Company Responsibilities as a Business Associate of a Covered-Entity

When a Customer is a HIPAA covered-entity and the Company requires access to HIPAA PI to perform contracted services, unless otherwise specified in a formal agreement between the Customer and the Company, the Company is responsible for:

- Adhering to the terms of formal Customer Agreements.
- Managing the access of Company and Third-Party Company Asset users to Customer Assets and PI.
- Monitoring Company and Third-Party Company Asset users with access to Customer Assets and PI to ensure that they adhere to Company [Acceptable Use](#) rules and access/use PI exclusively for the purposes defined in Customer agreements. See [Routine Monitoring and ISP Compliance Evaluations](#).
- Leveraging technologies, practices, and safeguards that align with the NIST CSF and comply with Customer data security and privacy policy.
- Directing all requests for access to, or challenges to the accuracy of, Customer Assets and PI (i.e. from Customer End-Users of all types) to the Customer for handling.
- Forbidding and protecting against the sale, use, or disclosure of Customer PI by the Company or Third-Parties for marketing or commercial purposes.
- Performing [routine risk assessment](#) and updating the Company ISP and ISP implementation as necessary to mitigate new/changed risk.
- Monitoring Company and Third-Party compliance with the Company ISP.
- Promptly notifying impacted Customer(s) of any breach or unauthorized release of Customer PI no later than seven (7) calendar days after discovery of a breach. See [Incident Response Plan - Breach Notification](#).
- Cooperating with the Customer and law enforcement to protect the integrity of investigations regarding breach or unauthorized release of PI.

## NYS Social Security Number Protection

In addition to standard security and privacy related roles and responsibilities, the Customer and Company have additional responsibilities to protect the security and privacy of Social Security Numbers in their custody.





## Customer Responsibility Under NYS SS# Protection Law

Unless otherwise specified in a formal agreement between the Customer and the Company, the Customer is responsible for:

- Only requesting, using, and retaining social security numbers (including not only the nine-digit number issued by the Social Security Administration but also "any number derived from such number") unless the number is encrypted as allowed.
- Granting Social Security Number access in Customer Records to only those Customer End-Users who need access to this PI to perform their job(s).
- Training Customer End-Users about acceptable and prohibited use of social security numbers.
- Monitoring Customer End-Users with Social Security Number access to ensure that Social Security Numbers are not being used in a prohibited manner.
- Ensuring that historically-retained Customer Assets comply with legislation as necessary.
- Notifying Customer End-Users impacted by security breach involving PI, regardless of fault in the breach, as required.
- Participating in and supporting formal investigations by law enforcement to the degree they are required under state and federal laws.

## Company Responsibility Under NYS SS# Protection Law

Unless otherwise specified in a formal agreement between the Customer and the Company, the Company is responsible for:

- Granting Social Security Number access in Customer Assets to only those Company and 3<sup>rd</sup> Party Company Asset Users who need access to this PI to perform their job(s).
- Training Company and 3<sup>rd</sup> Party Company Asset Users about acceptable and prohibited use of social security numbers.
- Monitoring Company and 3<sup>rd</sup> Party Company Asset Users with Social Security Number access to ensure that Social Security Numbers are not being used in a prohibited manner.
- Providing a means within Company Services for Customers to grant and revoke the access of specific Customer End Users to Social Security Numbers.
- Implementing and monitoring the compliance of the Company ISP, including [Administrative Safeguards](#), [Physical Safeguards](#), and [Technical Safeguards](#).
- Notifying Customers impacted by a Company security breach involving PI. See [Incident Response - Breach Notification](#).



- Participating in and supporting formal investigations by law enforcement to the degree they are required under state and federal laws.

## Information Security Procedures and Guidelines

The Company will adhere to all applicable general requirements, approaches, standards, implementation specifications, and maintenance requirements legislation governing PI in developing and maintaining policies and procedures for security standards for the protection of Company Assets, Customer Assets, and PI.

### Administrative Safeguards

#### Assigned Security Responsibility

The Company will identify a security official, known as the [Information Security Officer \(ISO\)](#), responsible for the adherence to this policy and to the implementation of procedures required to protect Company Assets, Customer Assets, and PI. See Information Security Roles and Responsibility section.

When there is a change in law that necessitates a change to the Company ISP policies and procedures, the ISO will document and implement the revised policies and procedures.

#### Risk Analysis

The ISO will perform at minimum a yearly risk analysis, which will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of Company Assets, Customer Assets, and PI.

Risk Analysis will leverage the downloadable Security Risk Assessment Tool (SRA) developed by the Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR).

- SRA Information and Download: <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>

#### Risk Management

Implementation of the ISP is the Company's primary means of risk management. Guided by the ISP, the ISO will define and oversee ITA/IT Team implementation of measures to reduce computer risks and vulnerabilities and to identify and respond appropriately to threats and violations.

#### Violations / Sanctions

In any incident that may be a violation of the Company's ISP, the role of the ITA/IT Team is to serve as investigators.

At the discretion of the ISO, incidents that are deemed unintended are documented and no disciplinary action taken. As determined by the Company ISO, single intentional actions or



repeat offenses are considered to be policy violations and will be handled in accordance with the enforcement actions described below.

- Company and Third-Party Company Asset Users who violate the Company's ISP may be subject to disciplinary action, up to and including dismissal/contract termination. Unauthorized access or disclosure of legally protected information may result in civil liability or criminal prosecution. For example:
  - Under federal law, violation of the HIPAA privacy rule may result in civil monetary penalties of up to \$250,000 per year and criminal sanctions including fines and imprisonment.
  - Under NYS Education Law 2d, entities with access to student PII and teacher/principal PII are liable for penalties associated with misuse or unauthorized release of such PI. The Educational Institutions tasked with guardianship of the PI may pursue legal action and reimbursement against those responsible for violations.
  - The New York Social Security Number Protection Law imposes severe financial penalties for the misuse or improper dissemination of Social Security numbers. The first violation of the law may result in a civil penalty of no more than \$1,000 for a single violation and \$100,000 for multiple violations. Any subsequent violation may result in a civil penalty of no more than \$5,000 for a single violation and \$250,000 for multiple violations.
- The Company may, without notice, temporarily or permanently suspend, block or restrict Company or Third-Party Company Asset Users' access to Company information and systems when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Company Assets, Customer Assets, and PI or to otherwise protect the Company.
- The Company may routinely monitor network traffic to assure the continued integrity and security of Company Assets, Customer Assets, and PI in accordance with applicable Company policies and laws. See [Routine Monitoring and ISP Compliance Evaluations](#).
- The Company may also refer suspected violations of applicable laws to appropriate law enforcement agencies.
- The Company will participate in and support formal investigations by law enforcement to the degree they are required under state and federal laws.

## Acceptable Use

Company Assets, Customer Assets, and PI must be used to conduct Company business and authorized activities. In this section the requirements of all Company and Third-Party Company Asset Users connecting or using the Internet through the Company network are defined. It is necessary to make sure that Company Assets, Customer Assets, and PI are properly used to avoid distractions in the work environment, and to avoid certain risks



including virus attacks, compromise of Company network systems and services, and legal issues.

This policy applies to all users, including administrative consultants, employees, contractors, administrators, and third parties that have access to Company Assets, Customer Assets, and/or PI.

### ***Prohibition of Personal Use***

Company Assets, Customer Assets, and PI may not be used by Company and Third-Party Company Asset Users for personal or unauthorized purposes.

Accessing and using information protected by State or Federal law (i.e. PI) is only permitted by explicitly authorized Company employees. Dissemination, discussion of, and/or use of PI outside of appropriate Company-approved, job-critical activities by Company employees is strictly prohibited, a violation of the Company's ISP, is sanctionable, and may require legal action to fully address.

### ***Electronic Mail and Instant Message Use***

Company and Third-Party Company Asset Users are prohibited from creating or sending electronic mail (e-mail) and instant messages:

1. that may be considered offensive or harassing, or that may contribute to a hostile environment;
2. that contains profanity, obscenities, or derogatory remarks;
3. that constitutes chain letters or spam;
4. to solicit or sell products or services that are unrelated to our business; or
5. to distract, intimidate or harass anyone, or to disrupt the workplace.
6. That contain PI

Company and Third-Party Company Asset Users are instructed to use caution when opening e-mail and attachments from unknown senders because they may contain viruses, root kits, spyware or malware.

### ***Social Media/Open Forums***

Online social networking sites and other online communication platforms and technologies are primarily aimed at personal relationships and communications among individuals. Company employees are prohibited from using social networking sites/services while at work unless authorized by the ISO.

When using social networking sites/services at home, Company employees should be mindful that whatever they publish may be accessible by members of the public long into the future and may be seen by the Company and its customers. The Company encourages employees to consider the following when writing or expressing themselves publicly:



1. Conduct themselves in a professional and businesslike manner, even if the communication is personal in nature.
2. Do not reference or discuss the Company's suppliers, vendors, customers, associates, contractors, potential business relationships or opportunities, competitors, or any entity that the Company does business with, or anything that might adversely impact the Company's business relationships.
3. Do not make statements about the Company's financial performance.
4. Do not use these media for Company marketing or public relations without Authorization.
5. When users are participating in social networking sites, users must be transparent that their thoughts are their own. Unless the Company officially designates the user, in writing, to speak or write for the Company, users should never state that they write or speak on behalf of the Company or that their viewpoints are the same as the Company, and users should make this clear to those reading or listening to their points of view. Users may consider a disclaimer to this effect, but note that it may not excuse improper or illegal conduct.
6. Do not disclose private, internal-use only, copyrighted, or confidential information belonging to the Company or third parties, including employees, associates, suppliers, vendors, competitors, customers, or any other person or entity that associates or does business with the Company. Such information includes personally identifying information (such as telephone numbers, Social Security numbers, credit or debit card numbers, or financial account numbers, etc.). Users should also not mention customers, vendors, potential business relationships or opportunities, or competitors in their social media activity. Users should use common sense and courtesy, and should follow strictly the Company's policies on protected information.
7. For social networking sites such as LinkedIn where personal and professional references are the focus: If users are representing themselves as a Company employee, users may not provide professional references about any current or former employee, contractor, vendor, or contingent worker. Users may provide a personal reference or recommendation for current or former Company employees, contractors, vendors, and contingent works provided (1) the statements made and information provided in the reference are factually accurate, and (2) users include the disclaimer "This reference is being made by me in a personal capacity. It is not intended and should not be construed as a reference from Company or any of its affiliated entities."
8. What users write or say, and how users write or say something, is up to each user. However, the Company provides notice that it reserves the right to read what users write or say publicly and make a determination if it meets the professional standards of the Company or damages the Company. Written or stated comments harmful or damaging to the Company or to its employees, associates, suppliers, vendors, customers, or any other person or entity that associates or does business with the Company may lead to immediate termination. This provision does not in any way



restrict users' right to engage in protected activity under Section 7 of the National Labor Relations Act.

9. Do not use vulgar, obscene, offensive, threatening, harassing, or defamatory language. Offensive language or content would include, but is not limited to, discrimination, harassment, or hostility on account of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic. Offensive language or content also includes soliciting sex or otherwise violating the laws regarding minors and their protection. Users that violate child protection laws, including solicitation of sex from minors, or posting of illegal pornographic material, will be subject to discipline including, but not limited to, termination.

## Information System Activity Review

The ISO, supported by the ITA/IT Team, will periodically review information system activity records—including audit logs, access reports, and security incident tracking reports—to ensure that implemented security controls are effective and that Company Assets, Customer Assets, and PI have not been potentially compromised.

Both Company and Third-Party Customer Asset Users are in scope for information system activity reviews.

Measures will include:

1. Enabling logging on computer systems managing Company Assets, Customer Assets, and/or PI.
2. Developing a process for the review of exception reports and/or logs.
3. Developing and documenting procedures for the retention of monitoring data. Log information should be maintained for up to six years, either locally on the server or through the use of backup tapes.
4. Periodically reviewing compliance to the Company ISP.

Customers are responsible for monitoring the activity of Customer End-Users accessing Customer Assets and PI. If the Company, in the course of its own security monitoring, determines that Customer End-User behavior in the system poses a significant threat to the operation or security of the system, Company Assets, Customer Assets, and/or PI, they will notify the Customer to whom the End-User belongs and take immediate appropriate action to correct the problem. See [Incident Response Plan](#).

## Workforce Security

The ISO will establish and communicate via the ISP procedures that ensure only authorized personnel have access to systems that manage Company Assets, Customer Assets, and PI.



## ***Employment and Access to Company and Customer Assets, and PI***

The Company provides email, collaboration tools, and access to other services and resources to facilitate the work of each employee for the benefit of the Company. It is the expectation and requirement of all employees to use the secure Company-provided and Company-approved technology resources for the transmission, storage, and processing of data and information related to and managed by the Company, including Company Assets, Customer Assets, and PI. The Company reserves the right to assign, review, access, and withdraw access to these tools and services, or to alter or modify access, based on employment role(s) and the interests of the Company.

Company employees are issued service accounts, security codes, keys, and other Company Assets when hired. Company-issued Assets shall be used for Company business.

Company employees are required to:

- Successfully pass applicable employee-vetting procedures during the hiring process (e.g. required documentation, reference checks, background check, certification confirmation, etc.)
- Maintain required certifications / qualifications for the duration of their employment.
- Acknowledge and comply with all terms of the Company ISP.
- Complete all Company-required training.
- Acknowledge and comply with all updates to the Company ISP during the full term of their employment with the Company.
- Exercise good judgment in maintaining the security of all Company Assets, Customer Assets, and PI.
- Only access Company Assets, Customer Assets, and PI to which they have been explicitly authorized, whether or not the Company Assets are physically or technically protected from access.

## ***Privileged Users***

Some individuals (including both Company or Third-Party Asset Users), by virtue of their role or position, have unusually broad access to information, manage systems and services on behalf of the Company, or otherwise have elevated privileges in some area of Company business. Such individuals, upon leaving the position resulting in elevated privilege, will be assigned privileges and services appropriate to the new role, and unnecessary privilege and service access will be removed. This is done not as a punitive measure but as a protection for both the Asset User and the Company. The decision to assign new privileges and access to data/information and services is at the sole discretion of the Company.

## ***Changes of Role or Position***

When Company or Third-Party Asset Users change roles, such changes may not immediately be reflected in their access to files and systems. When such a transition occurs, and the Asset



User finds that access from their prior role persists, the Asset User shall promptly notify both their current and previous supervisor. Until the appropriate changes have been made, the Asset User shall make use only of that access appropriate to their current role.

Supervisors, both in the Company and in Third-Party Organizations with Company Asset Access, are required to ensure that Asset Users transitioning between roles are assigned only appropriate access.

### ***Departing Employment***

Company resources are provided for the benefit of the Company. When an individual leaves the Company's employ, voluntarily or otherwise, access to such resources will be curtailed. It is incumbent on the departing employee to appropriately transfer access to any resources not already available to the department, and to ensure that supervisors have the necessary authorization to ensure business continuity.

Any mail or messages (electronic or paper), contacts, associated attachments or documents used in the operation of Company business are to remain under the domain and control of the Company upon employee separation. Email addresses used by departing employees may be repurposed or decommissioned at the discretion of the Company.

- **Departing Company Employees (Company Asset Users)**  
It is the responsibility of the ISO, with the support of the ITA/IT Team, to ensure that all departing employee access is terminated in 24 hours or less after the effective termination date, removing the departed employee's access to Company Assets, Customer Assets, and PI.
- **Departing Third-Party Employees (Third-Party Company Asset Users)**  
It is the responsibility of Third-Party Organizations with Company Asset Access (granted by the ISO by virtue of a formal agreement with the Company) to ensure that all departing employee access is terminated in 24 hours or less after the effective termination date, removing the departed Third-Party Asset User's access to Company Assets, Customer Assets, and PI.

### **Information Access Management**

The ISO will establish procedures in compliance with the Company ISP to be deployed and managed by the ITA/IT Team that ensure that all systems that manage Company Assets, Customer Assets, and/or PI have authorization controls that allow only those with appropriate authorization.

Customers, BOCES, and Colleges/Universities with access to Company Services are responsible for their own information access measures beyond those that are native to Company Services.





## Security Communication, Awareness, and Training

### *Acceptable Use Rules*

[Acceptable use rules](#) stipulate constraints and practices that Company and Third-Party Company Asset Users must agree to for access to Company Assets, Customer Assets, and PI. The ISO will maintain and disseminate Company Acceptable Use rules and track formal acknowledgement/acceptance of the rules.

### *Security Training and Routine Communication*

The ISO will ensure that the ITA/IT Team, Company Asset Users, and Third-Party Company Asset Users (as appropriate) receive routine security refreshers, updates, and training related to the Company ISP so that they remain aware of, and may remain in compliance with, the latest Company Asset, Customer Asset, and PI policy and protection requirements, for example:

- ISP Change/Update Notifications
- Acceptable Use Training
- PI Access, Usage, and Handling Training (includes HIPAA, Ed Law § 2-d, and Social Security Numbers)
- Mobile Security and Privacy Training
- Data Storage, Transmission, Retention, and Destruction Training

### *Non-Disclosure & Protection of Sensitive Security Information*

Sensitive security information (“SSI”) is information that, if publicly released, could be used to breach/exploit/access without authorization Company facilities or systems. The following information constitutes SSI:

- Security Programs and Contingency Plans
- Security Directives
- Performance Specifications
- Vulnerability Assessments
- Security Inspections or Investigative Information
- Threat Information
- Security Measures
- Security Screening Information
- Security Training Materials
- Identifying Information for Security Personnel



- Information about Security-Related Vendors Serving the Company
- Critical Infrastructure Asset Information
- Systems Security Information
- Confidential Business Information
- Research and Development
- Software Source Code, Architectural Information, Schemas, etc.
- Other Information as Determined by the Company Information Security Officer

As persons creating or receiving Company SSI in order to perform functions of their job, Company employees (and, as applicable, contractors) must protect this information from disclosure to those outside the Company as well as those within the Company (or Contracted Organization) that do not need to know the information to do their jobs.

## Password Management

### *Passwords Used by Company and Third-Party Company Asset Users*

A secure network environment requires all users to use strong passwords. Password standards help prevent the compromise of user accounts and administrative accounts by unauthorized users who use manual methods like social engineering or automated tools to guess weak passwords. All employees will adhere to the following guidelines regarding passwords on systems managing ePHI, as they are stronger than HIPAA requirements:

1. Use passwords, which have at least eight characters and include a combination of both capitalized and lower-case letters, numbers, and symbols.
2. Avoid use of repetitive or sequential characters (e.g., aaaaaa or 1234abcd)
3. Avoid use of context-specific words, such as the name of the service, the username, and derivatives thereof (e.g. mattsemailpassword56!)
4. When changing a password, do not reuse any old passwords or simply append a previously used password.
5. All possibly impacted passwords should be changed following a suspected or known breach.

### *Passwords Used by Customers, BOCES, and Colleges/Universities*

Password policies in Company Services are configurable. Customers, BOCES, and Colleges/Universities are responsible for defining password policies and enforcing them in Company Services with proper account configuration.



## Security Incident Procedures & Reporting

### *Security Incident Notification Procedures*

#### *Internal Incident Reporting*

All users are accountable for reporting any suspected data breach of the Company Network to the ISO, either directly or via the ITA/IT Team.

Incidents can be communicated via the “SUBMIT A TICKET” link at <https://support.schoolfront.com/home/> or via email address, <mailto:abuse@schoolfront.com>.

#### *External Incident Reporting*

Confirmed or suspected security and privacy issues can be reported to Company leadership by anyone inside or outside the Company. Incidents can be communicated via the “SUBMIT A TICKET” link at <https://support.schoolfront.com/home/> or via email address, <mailto:abuse@schoolfront.com>.

Information and instructions for reporting security and privacy concerns are available publicly in the following locations:

- SchoolFront Website: <https://www.schoolfront.com/privacy-security>
- RecruitFront Website: <https://www.recruitfront.com/terms-policies>

### *Security Incident Reporting (Documentation) Procedure*

When a security incident occurs, documentation is required for compliance. The ISO is responsible for creating, maintaining, and storing this documentation.

#### *Creating an Incident Report*

Whenever an incident is reported, whether from an internal source (e.g. an employee) or external source (e.g. a customer), an incident report must be generated and include the following information:

- Unique Identifier (used to track related documentation, e.g. the [security log entry](#))
- Contact Information
- Security Incident Description
- Impact/Potential Impact
- Sensitivity of Information/Information Involved
- Severity Rating (i.e. a severity rating from 1 to 5, with 1 being the most serious and 5 being the least serious)
- Notification
- Incident Details
- Mitigation



- ISO Signature

### ***Security Incident Report Retention***

The ISO, on behalf of the Company, is responsible for retaining all security incident reports and security incident logs for at least six (6) years.

### **Incident Response Plan**

The purpose of the Company's Incident Response Plan (IRP) is to provide guidance on the appropriate steps to be taken and documented in the event of a possible security incident or data breach, from the time of suspected breach to post-incident response closure, so that all incidents are handled in a consistent manner and the exposure to the potentially breached party is limited. It also provides a methodology for collecting evidence in the event of criminal activity. Documentation of responsive actions taken in connection with any security incident or data breach, as well as documentation of the post-incident events and actions taken, is critical in making appropriate changes to business practices to improve the safeguarding and handling of Company Assets, Customer Assets, and/or PI.

#### ***Incident Response Process - Initial Discovery***

1. Anyone suspecting or noting a security incident, data breach or potential system compromise, or malicious activity contacts the ISO.
2. The ISO, with the support of the ITA/IT Team, will determine if there has been a security incident, and the nature and seriousness of the incident, by considering the following questions:
  - a. Does the system contain Company Assets, Customer Assets, and/or PI?
  - b. Is there a chance outside law enforcement may need to get involved?
  - c. Is there a requirement or desire to perform a forensics analysis of the system compromise?

If the answer is "yes" to any of these questions then immediately coordinate actions to be taken and apply the below as appropriate.

If the answer is "no" to all the questions, then apply the below as appropriate.

#### ***Incident Analysis and Corrective Action***

The ISO, with the support of the ITA/IT Team, will:

1. Do preliminary analysis - isolate the compromised system by disconnecting the network cable. If this is not feasible or desirable, Information Security can block access to the compromised system via the network.
2. Determine the security incident type—i.e. Try to determine the cause of the malicious activity and the level of system privilege attained by the intruder and implement appropriate remedial measures.



If a system is compromised the ISO, with the support of the ITA/IT Team, will:

1. Disable any compromised accounts and terminate all processes owned by them.
2. Compile a list of IP addresses involved in the incident, including log entries if possible, and forward the data to Information Security.
3. Determine the employees (and any other users) that need to change their passwords due to the compromise, as well as whether or not they have accounts on other systems using the same credentials and advise that they change passwords on those systems.
4. Notify the owners of the compromised accounts and reissue credentials. Consider the likelihood of the intruder having access to the compromised account email and utilize other contact methodology.
5. Determine whether all affected users have established new user IDs and passwords (if applicable).
6. Rebuild the system, and verify that its network access should be re-established (if applicable).
7. Perform a network vulnerability scan of the system after it is unblocked to identify any unresolved security issues that might be used in future attacks against the system.

### ***Post-incident Lessons Learned***

After corrective measures are completed, the ISO will:

1. Review chronology of the event.
2. Identify what went wrong and what went right.
3. Identify the threat or vulnerabilities that were exploited and determine whether it/they can be alleviated.
4. Review if all intrusion detection or prevention was in place, active and up to date.
5. Formally document the incident and “lessons learned” and assign appropriate updates to ISP.
6. Disseminate, as appropriate, the incident documentation and lessons learned.

### ***Incident Response - Breach Notification***

If a security incident is suspected to be a data privacy breach, the ISO will immediately notify the Company CEO and General Counsel.

The ISO, with the support of the ITA/IT Team, will:

1. Determine what information was suspected to be breached, i.e., specific individuals' first and last names with a type of Company Assets, Customer Assets, and/or PI.



2. Identify the scope, time frame and source(s) of breach, type of breach, whether data encryption was used and for what, possible suspects (internal or external, authorized or unauthorized, employee or non-employee user).
3. Bring in an incident response expert or law enforcement to conduct an investigation (as necessary and appropriate).
4. Review for other compromised systems.
5. Monitor all systems for potential intrusions.
6. Determine the notification requirements (statutory or contractual) and address within the required timeframe.  
See, for example, [Company Responsibilities Under NYS Education Law § 2-d](#).

## Routine Monitoring and ISP Compliance Evaluations

The ISO will perform at minimum an annual review/evaluation of compliance with the Company's ISP, as well as the following routine monitoring activities:

### ***System Access Reviews***

The ISO with support from the ITA/IT Team, will periodically review the accounts on systems managing Company Assets, Customer Assets, and/or PI to ensure that only currently authorized persons have access to these systems.

### ***Company Asset and PI Access and Usage Monitoring***

By accessing/using Company Assets (including accessible Customer Assets and PI) provided by the Company, Company and Third-Party Company Asset Users agree to adhere to the Company ISP and acknowledge that logs of Internet access, such as sites visited, images reviewed, and email sent, may be recorded and monitored by the Company at any time with no expectation of privacy and that:

1. Encrypted technology that meets ISP requirements will be employed.
2. The Company owns the rights to all Company Assets and will take necessary measures to protect Company Assets, Customer Assets, and PI, subject to applicable laws.
3. Company and Third-Party Company Asset Users may not access Company Assets to which the Asset User has not been granted authorization.
4. Company and Third-Party Company Asset Users may not destroy, delete, erase, or conceal Company Assets, Customer Assets, and/or PI.
5. Company and Third-Party Company Asset Users may not access another user's computer, computer files, or electronic mail without authorization from the ISO.
6. The Company licenses the use of certain commercial software application programs from third parties for business purposes. Third parties retain the ownership and distribution rights to this software. Company and Third-Party Company Asset Users may not distribute licensed software or use it for unauthorized (by the ISO) activities.



7. Email messages sent and received using Company equipment or Internet access provided by the Company are not private and are subject to viewing, downloading, inspection, release, and archiving by the Company.
8. The Company has the right to inspect files stored in private areas of the Company network or on individual computers or storage media to assure compliance with the Company ISP and applicable state and federal laws.
9. The Company may monitor electronic mail messages (including personal/private/instant messaging systems).
10. The Company may use software to monitor messages, files, or other information that is entered into, received by, sent, or viewed on Company's network, devices, resources, and services.

### ***Access to an Employee's Device or Files***

If the ITA/IT Team determines that employee files or messages pose a significant threat to the operation or security of a Company computer, system, Company Assets, or PI, they will take immediate appropriate action to correct the problem. Additionally, the ITA/IT Team may restrict the employee's access to that computer or network system.

If possible, the ITA/IT Team should consult with the ISO prior to taking action. As soon as possible after action is taken, but no later than the next business day, the ITA/IT Team will make a written report to the ISO outlining the nature of the situation, including, but not limited to:

1. the nature of the threat
2. protective actions taken
3. the employee(s) involved
4. the employee files or messages that were affected

The ISO will evaluate the situation and make a determination as to whether a violation of the Company ISP has occurred, and how the violation will be handled.

### ***Administrative Access by System or Network Administrators***

The Company reserves the right to examine all Company-owned and Company-operated computer systems and electronic/digital resources, as well as authorized employee-owned devices connected to Company networks. Unauthorized devices are not allowed to be used to access Company Assets, Customer Assets, and/or PI.



## Physical Safeguards

### Environmental Access Controls and High-Availability

The ISO, supported by the ITA/IT Team, will ensure that systems that manage Company Assets, Customer Assets, and/or PI are kept in areas with physical security controls that restrict access but support high-availability.

#### *Data Center Facility*

All production Company hardware and systems are Company-owned and maintained, and housed in a highly secure, Class A Data Center in Rochester, NY with features designed to ensure high-availability of Company Assets (e.g. systems and services).

- **Security** - Access is permitted by authorized personnel with different levels of entrance security. On-site security personnel monitor all perimeter doors, security alarms, and digital surveillance video cameras which monitor and record entry and exit to prevent unauthorized activity. The Company has direct access into the facility 24 hours a day, 365 days a year with biometric authentication.
- **Power Protection** - The data center provides continuous power 24 hours a day, 7 days a week. Power protection is provided through multiple uninterruptible power supplies with battery backup to ensure a clean and stable supply of power. Emergency diesel power generators are automatically activated in the event of a power disruption.
- **Environmental Control** - The data center is equipped with redundant, independent cooling units. Temperature and humidity are electronically controlled through sensitive moisture sensors.
- **Fire Detection and Suppression** - Fire suppression in the data center is provided through systems on the floor and ceiling, monitored by a multi-zone smoke and fire detection system.
- **Raised Floor** - The data center uses 18-inch raised floors to accommodate cabling and cooling.
- **Cabling** - Category 5e & 6 or optical fiber cabling with Gigabit Ethernet capabilities. Cables are routed under the raised floor in protective cable trays to ensure a traceable, secure cable route.
- **Physically Locked Cabinets/Cages** - All Company Assets are secured within physically locked cabinets/cages within the secure data center.

#### *FrontEdge Office / Headquarters*

- Building/Office Security -
  - **Locks and Access Logging** - The Company office/headquarter at 274 North Goodman Street, Suite B265, Rochester, NY 14607 is protected by physically locked doors, requiring programmed keys to unlock. Keys are assigned to



employees when they are hired. All access to the Company office/headquarters is logged for monitoring and auditing purposes. Keys are disabled and returned when employees depart the company.

- **24/7 Security and Fire Monitoring** - The office is monitored 24/7 by a professional security firm and linked directly to police and fire services in the event of an emergency such as a break-in or fire. Wired control panels used to arm and disarm the system are installed at entrances. Employees are assigned individual security codes for arming and disarming the security system when they are hired. Codes are decommissioned when they depart the company.
- **Production Information Systems** - All production Company hardware and systems are housed in a highly secure, Class A Data Center in Rochester, NY with features designed to ensure high-availability of Company Assets (e.g. systems and services). Data center systems are accessible both physically and remotely (i.e. from the Company Office/Headquarters or off-site employee workstations) only by authorized personnel.
- **Workstations** - See [Standards for Company Computers](#) and [Work Station Use](#) and [Workstation Security and Availability](#)
- **Non-Production IT Environments** - Non-production IT environments (e.g. development, test, staging, etc.) are both physically secured (e.g. with locks or within locking cabinets/storage areas) and technically secured. (See [Standards for Company Computers](#))

## ***Mobile / Remote Workers***

### ***Working Off-Site***

The physical and logical controls that are available within the Company environment are not automatically available when working outside of that environment. There is an increased risk of information being subject to loss or unauthorized access. Mobile computing users must take special measures to protect sensitive information in these circumstances.

Removal off-site of any Company Assets, Customer Assets, or PI (i.e. on laptops, mobile devices, or storage medium) must be authorized by the ISO. Prior to authorization a risk assessment should be carried out by the ISO, to protect against loss or unauthorized access, and appropriate risk management processes put in place. The risk assessment must take into account the sensitivity of the Company Assets, Customer Assets, and PI.

Company and Third-Party Company Asset Users accessing information systems remotely to support business activities (including from home PCs) must be authorized to do so by the responsible information owner. Prior to authorization a risk assessment should be carried out and appropriate risk management processes put in place. The risk assessment must take into account the sensitivity of the information.

Laptops and home personal computers should not be used for business activities without appropriate security measures, including up to date security “Patches” and virus protection and encryption. (see [Antivirus/Malware/Security Patches](#))



When undertaking mobile computing the following guidelines must be followed:

1. When travelling, equipment (and media) must not be left unattended in public places. Portable computers should be carried as hand luggage when travelling.
2. When using a laptop, do not process personal or sensitive data in public places e.g. on public transport. Or public Wi-Fi unless ensuring all transmitted data is encrypted.
3. Passwords or other access tokens for access to the Company's systems should never be stored on mobile devices where they may be stolen or permit unauthorized access to information assets. For example, options to automatically "remember" passwords should not be accepted. Passwords and passkeys should not be saved on the mobile device.
4. Security risks (e.g. of damage, theft) may vary considerably between locations and should be taken into account when determining the most appropriate security measures.

When working with other organizations (e.g. a BOCES supporting a Company product or at a customer facility), make sure that the employee complies with the organizations guidelines relating to mobile computing.

See also [Mobile Device Security](#).

### ***Non-Company Networks***

As part of the risk assessments described above, employees must take account of the risks associated with using wireless networks and non-Company networks. Sensitive data or information may only be transferred across networks when the confidentiality of the data or information can be assured throughout the transfer.

The following should be noted:

1. Wireless networks and public networks are less secure than the Company's private, wired network environment.
2. Email is an inherently unsecure way of transferring sensitive information and should be used with caution.
3. Where there is no alternative to transferring/accessing sensitive information across unsecure networks or by email, advice should be sought on appropriate steps to protect the information. The Company's ISO will advise on appropriate mechanisms for the secure transfer of sensitive information, particularly outside of the Company's secure environment.

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. We reserve the right to advise appropriate authorities of any violation of law.

The ISO is responsible for ensuring compliance with the Mobile Computing Policy and the controls created to safeguard the Company and its assets.



Any exceptions must be approved by the ISO.

### ***Mobile Device Security***

See Also [Mobile Device Security](#)

### **Workstation and Mobile Device Use**

The ISO, supported by the ITA/IT Team, will ensure that only designated workstations possessing appropriate security controls will be used to access and manage ePHI, and that these workstations are not used in publicly-accessible areas nor used by multiple users not authorized to access ePHI. This security measure extends to the use of laptops and home machines. See [Mobile Device Security](#).

### ***Standards for Company Computers***

#### ***Standard Company-Issued Image / Configuration***

Unless exempted by the Company ISO, computers must use the Company-issued image without alteration, including:

1. Authorized operating system and version
2. Encryption appropriate to device
3. Company provided antivirus, set to auto update
4. Local firewall enabled
5. Monitored patch management
6. Authorized VPN installed
7. Backup managed by Company
8. No local administrator accounts

Only Company-issued, secure computers and laptops or those explicitly reviewed and authorized by the ISO may be used to access Company Assets, Customer Assets, and PI.

Devices used to conduct Company business may be assessed for compliance at the discretion of the Company. See [Company Asset and PI Access and Usage Monitoring](#). The Company reserves the right to examine all Company owned and operated computer systems and electronic/digital resources, or any such devices used to conduct Company business or making use of the Company's network and technology resources. The Company will take any/all necessary measures required in addressing actual or potential compromise or threat to Company Assets, Customer Assets, and PI.

#### ***Antivirus/Malware/Security Patches***

The ISO is responsible for ensuring that Antivirus and Malware Policy and Procedures are followed.

Computing Assets

1. The willful introduction of a computer virus, malware, and disruptive/destructive code to the Company Network is prohibited.
2. Users are not to make any changes to their system that will disable or remove Company approved antivirus and malware prevention software or otherwise prevent the software from performing its intended purpose.
3. Users are not to open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. All unexpected content received from a trusted source should be verified with that source prior to opening. Users who discover or suspect virus or malware incidents must report them without delay to the ISO and await further instructions. See [Incident Procedures and Reporting](#).
4. Computer systems that are unable to run antivirus and malware prevention software must be restricted to an isolated network with sufficient network-level protections deployed to prevent viruses/malware from spreading into any other areas of our network (e.g., running antivirus technology at its “gateway” to the Company Network).
5. Automatic update frequency cannot be altered to reduce the frequency of updates.

#### Installation, Management, Maintenance and Support

1. The ITA/IT Team is responsible for deploying and maintaining approved antivirus/malware prevention software to all systems it supports/administers and for providing timely updates for all components of the software on:
  - any externally facing servers or gateways;
  - proxy servers;
  - application servers such as mail servers and/or mail gateways, FTP servers, web servers, audio/video servers;
  - data management servers such as back-up servers and database servers;
  - Company deployed desktops, laptops, and tablets;
  - when technically feasible, cell phones, smart phones and PDAs; and
  - for non-Company deployed laptops or mobile devices, Information Technology should ensure that both up-to-date antivirus/malware prevention software and a personal firewall are deployed on the connecting device prior to granting permission to connect to the Company Network.
2. Antivirus/malware prevention updates will be installed and scheduled to run at regular intervals or upon electronic notification of a new security update, patch, vulnerability, or threat. Wherever possible, our computing resources should be set to auto-apply/update security patches on a regular basis.
3. Antivirus and malware prevention scanning should be programmed to run/initiate upon startup and/or reboot of PCs/servers/other computing devices.



4. For PCs/servers/computing devices that are not normally rebooted, antivirus and malware scanning should be “always on” when technically feasible. If not possible, Information Technology should ensure that antivirus and malware remediation is accomplished for the protection of our electronic assets.
5. The ITA/IT Team is responsible for receiving and acting upon alerts (via automated alert, email, news, etc.) promptly to ensure minimal exposure and security risk to the confidentiality, integrity, and availability of our electronic assets.
6. Critical security patches should be deployed by ITA/IT Team a maximum of 48 hours after release by the operating system software or application vendor, unless there is reason to believe the patch might negatively impact a business-related activity or application.
7. After appropriate testing, updates without issue will be made available to all PCs/servers/computing devices, as well as to devices utilized by remote employees.
8. The ITA/IT Team will run malware prevention software scans routinely (at a minimum weekly).
9. The ITA/IT Team will run antivirus and malware prevention software immediately after the installation of any new software, not normally supported by the ITA/IT Team.
10. Suspicious content (files or macros attached to email) should be quarantined for review or permanently deleted immediately.
11. All downloads should be scanned with an updated Company standard antivirus/malware prevention scanner immediately (automatically, if possible).
12. Computing systems will be rebooted as required to ensure virus definitions (as well as operating system updates) are updated and that the antivirus software can run to check for viruses.
13. Default settings should be set up so that antivirus software runs upon startup or reboot.

### ***Workstation Security and Availability***

The ISO, supported by the ITA/IT Team, will ensure that physical safeguards are in place to protect workstations that access and manage Company Assets, Customer Assets, and PI are consistent with the Company ISP.

See [Standards for Company Computers](#).

### ***Company Service Security and Availability***

Company Services (e.g. SchoolFront, RecruitFront, hosting, etc.) are available and fully accessible to Customer End-Users, BOCES Users, RecruitFront Applicants, etc. via the World Wide Web twenty-four (24) hours per day, seven (7) days per week, with the sole exception of scheduled maintenance periods, which, unless otherwise communicated by the Company,



shall last no longer than 1.5 hours per week and shall be scheduled between the hours of Saturday at 11:00 p.m. and Sunday at 4:00 a.m., Eastern time. Maintenance periods allow the Company to perform general maintenance on Company Assets and is a critical part of Company risk mitigation.

### ***Mobile Device and Remote Access Security***

This section establishes guidelines, where technically feasible, governing the secure and safe use of mobile devices. The same standards applied to Company computers (i.e. workstations, servers, etc.) should be applied to mobile devices. See [Standards for Company Computers](#).

Additional standards and rules must be followed by mobile device users accessing Company Assets, Customer Assets, and PI and employees accessing Company Assets, Customer Assets, and PI outside of the Company-controlled environment (i.e. the Company office/headquarters and from within the Data Center) where Company-managed physical and logical controls are not automatically available:

1. Shipments of new or unassigned Devices are to be stored, within a reasonable time of receipt, in locked closets or rooms with secure, controlled access.
2. Security instructions to users should be included with Device checkout.
3. A locking cable to secure the Device to a large stationary object, such as a desk or airplane seat, will be issued upon request or as needed with each Device, except smartphones.
4. In “open” access areas, a laptop restraint/lockdown device will be used when the computer is left unattended if deemed necessary to protect it.
5. Identification labels with the Company name/ID shall be visibly placed on all laptops to assist in identification if stolen or misplaced. Please note that where a safety issue is involved, the local security environment may necessitate masking the Company name.
6. The Device make, model, serial number, and media access control address is to be recorded and stored in a safe location to give precise information to authorities in case of theft.
7. The Information Technology Department (“Information Technology”) is responsible for assuring that all Devices owned by the Company have the most recent software and hardware configuration and available upgrades installed.
8. Unattended storage standards for Devices should be the same as those for the storage of similar hard copy information.
9. Back-ups of Company data onto Company servers should be accomplished on a basis which ensures their availability and negates the significant loss of such data.
10. Sensitive data stored on laptops and other mobile devices should be kept to a minimum to reduce risk and impact should a breach of security occur.

11. The user has overall responsibility for the confidentiality, integrity, availability, and accessibility of his/her assigned Company device, and the data on or accessible through the Device.
12. Encryption to maintain confidentiality and protect against the bypass of software controls (e.g., booting from a system disk or USB, file encryption) must be utilized. Encryption will be used when sending and receiving Company Sensitive Information or PII.
13. Anti-virus/anti-malware software will be installed on the Device and all incoming disks/magnetic/digital media /jump drives should be virus-checked before being used.
14. Users must take steps to prevent casual overview or attempted use by unauthorized personnel. The use of privacy screens is encouraged.
15. User ID and authentication is required before access is given to data and applications residing on the Device. Some smartphones only allow for pattern or PIN for authentication without a User ID, which is acceptable for accessing the Device itself.
16. Users are responsible for taking reasonable precautions to protect and maintain Devices. Evidence of misuse or abuse of a Device may result in the revocation of the user's use of such Device.
17. A screensaver and password or "clear and lock" feature will be used to protect the Device if the user must leave the activated Device; a user password must be re-entered for further access.
18. Mobile devices are vulnerable to theft, loss or unauthorized access when taken outside of the Company's physical environment. They must be provided with appropriate forms of access protection to prevent unauthorized access to their contents:
  - a. Password protection must be in place, while recognizing that passwords offer only limited protection against a determined attack.
  - b. Time-out protection (e.g. screen saver or hibernation with password) must be applied.
  - c. Where sensitive information is held on laptops or mobile storage devices, data encryption must be applied to that information or to the entire device.
  - d. Full device encryption offers the maximum protection for sensitive information on laptops and other devices and should be used where the sensitivity of data requires it. Alternatively, and where appropriate, data can be encrypted at the partition level or virtual partition (a file encrypted to behave like a disk partition) level. In most cases, encrypted virtual partitions or disks can be copied to USB pens, CDs and DVDs for safe transportation. Note that data is only protected by encryption when the laptop is powered off and not in normal use.



- e. Access to encrypted information is lost if the encryption key is forgotten. Users should ensure that a secure, unencrypted backup copy of encrypted information is retained on central systems.
  - f. The Company’s ISO will offer advice on encryption products, options and configuration.
19. To help prevent damage and theft, a laptop should not be placed in or as checked baggage. If a laptop must be left in an automobile, it must be stored in the trunk or otherwise out of plain view.
  20. Losses are to be immediately reported to appropriate authorities, Loss Prevention and Information Security.
  21. Sensitive information held on any mobile device must be securely erased before the device is reassigned to another user or to another purpose. Where necessary, advice should be sought from the Company’s ISO on appropriate tools for erasing information on PCs and mobile devices.

***Information Security Guidelines for Domestic and International Travel***

The chance of an information security compromise while traveling is small but the impact of a compromise can be significant. Following best practices helps to reduce the likelihood of an exposure and minimizes the impact should an exposure take place.

Foreign universities, governments, and companies are often intricately linked. Any inquiry by any person may have an ulterior motive, such as stealing intellectual property or accessing PI. Be cautious of unsolicited requests and questions about the Company, Customers, your work, or other information, however innocuous-seeming.

	Domestic Travel	International Travel
<b>Before leaving</b>	Request authorization from the ISO to take Company Assets (including devices, accessories, and information) and IP off-site.	
	Remove any information not needed on trip.	
	Consider keeping all data on a Company server and accessing it only via a secure VPN connection. When possible travel with a "clean" device, containing only necessary applications and information for the trip.	
	Update equipment with the latest patches, updates, firewall and antivirus software.	
	Image device.	
	Encrypt all information.	
		Check the Export Administration Regulations (EAR) and International Traffic and Arms Regulations (ITAR)



		laws concerning any software on your computer that may be non-exportable or require licensing to take it out of the country. Remove all files containing controlled information or information involving restrictions.
	Be aware that your belongings maybe searched multiple times and electronic media copied. If you have sensitive intellectual property that might have commercial value or PI, avoid bringing it.	
	Complete any additional travel-preparation tasks required by the ISO when they authorized your travel with Company Assets and IP (e.g. the installation of tracking software).	
<b>While traveling</b>	Use a VPN to access Company resources.	
	Assume that any equipment other than your own is insecure. This includes equipment owned by friends, at cybercafes, in hotel business centers, libraries, etc. Do not enter sensitive information (e.g. credit cards, bank accounts, passwords) in Wi-Fi hotspots, or other insecure locations.	
	Always log-off of and lock devices and avoid leaving them unattended.	
	Data sticks/flash drives, CDs, PDAs, phones, etc., containing Company Assets and/or PI must be physically secured.	
<b>Upon return</b>	Scan for malware and remove if found.	
		Identify and extract information collected on trip.
		Wipe and re-image device. Do not copy sensitive information onto a computer that has been overseas and has not been inspected and cleared by the ITA upon return.
		Change passwords and always adhere to Company <a href="#">password</a> guidelines.

### Additional Considerations for Traveling Abroad

- All information you send electronically can be intercepted. Wireless devices are especially vulnerable. Hotel business centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched. Corporate and government officials are most at risk, but don't assume you're too insignificant to be targeted.



- Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this, remove the battery.
- Foreign security services and criminals are adept at “phishing” - that is, pretending to be someone you trust in order to obtain personal or sensitive information.
- Likewise, avoid using public charging stations. It can be nearly impossible to tell if a charging station is also accessing your phone's data. If unavoidable, one precaution is to power off your phone completely before connecting it to the charging station.
- Store hardware tokens, battery and SIM card in a separate location from the mobile device.
- Seek official cyber security alerts from: [www.onguardonline.gov](http://www.onguardonline.gov) and [www.us-cert.gov/cas/tips](http://www.us-cert.gov/cas/tips)

## Device and Media Controls

The ISO, supported by the ITA/IT Team, will ensure that procedures are in place to govern the receipt and removal of hardware and electronic media that contains PI into and out of a facility, and the movement of these items within the facility. Media can include hard disks, tapes, floppy disks, CD ROMs, optical disks, and other means of storing computer data.

### *Data Backup*

The Company takes backups of both Company data and Customer data (for the timeframe set forth in each Customer Agreement) including:

- Onsite encrypted database log backups taken every hour
- Onsite encrypted full backups taken nightly and copied to a secondary server
- Encrypted VM backups of entire servers taken nightly and synchronized offsite
- File backups taken nightly to secondary server
- Encrypted file backups taken nightly to cloud

The following Company encryption practices are in place:

- HTTPS for all web traffic
- SFTP for FTP traffic
- BitLocker for content at rest
- SQL encryption for subset of content within the database

### *Data Retention*

The Company's data retention policy, unless otherwise specified in a formal Customer Agreement, is as follows:



- Complete data backups, including those run hourly, are retained for 3 months.
- After 3 months and up to 6 months daily full backups are retained.
- After 6 months and up to 12 months Sunday full backups are retained.
- After 12 months, only backups conducted 1 Sunday per month are retained.

If a Customer requires data to be restored from a backup due to data loss caused by their own actions and not a resulting from a software bug, a onetime fee may be charged for data restoration. Customers are allotted unlimited data storage and retention for the timeframe set forth in each Customer Agreement. The Company does not currently require pruning of Customer Data housed in Company Services during the term of Customer agreements.

At the conclusion of a Customer agreement or in the event of agreement termination, Customer/BOCES and Customer End-User/BOCES User access to Company Services is removed via the elimination of the terminated Customer Account from active Company Services.

The Customer/BOCES is responsible for the retention of their own data (i.e. as required by law) beyond the term of their Agreement with the Company following Agreement termination or conclusion. It is the responsibility of the Customer to extract all data that they need from the system using the supplied grids and export to Excel for database content. File representation of personnel folders / files can be backed up to a district or BOCES server at a formally agreed to cadence leveraging the Company's Backup Service.

### ***Sanitizing Company Devices***

Devices are inventoried and when removed from service are "cleaned" with a US DoD 5220.22-M/NIST 800-88 disk cleaning solution. Certificates of cleaning are retained for 6 years.

## **Technical Safeguards**

### **Access Control**

The ISO, with support of the ITA/IT Team, will ensure that security controls are in place to protect the integrity and confidentiality of Company Assets, Customer Assets, and PI residing on computer systems, including applications, databases, workstations, servers, and network equipment using procedures associated with the Company ISP.

### ***Unique User Identification***

Unique user identification will be used in all Company Services and, where practical, to access Company physical location and physically-secured assets. User activity will be tracked and held accountable for access and usage that violates the Company ISP and PI laws.

### ***Emergency Procedures***

The ISO will establish, maintain, and communicate procedures for gaining access to Company Services and Assets, including PI, in the event of an emergency. Procedures for Customer



access should be included for types of emergencies impacting Customer access to Customer Assets and PI.

All Company workstations and Company-outfitted devices are configured for automatic log-off requiring password authentication for re-access when left unattended to prevent unauthorized users from accessing Company Assets and PI during an emergency wherein users are required to immediately leave.

Company Services, like SchoolFront, support log-off rules which can be defined and configured by Customers so that the Service times-out and requires re-authentication after a configured period of time.

### ***Encryption and Decryption***

See [Device and Media Controls](#) and [Transmission Security](#)

### **Audit Controls**

The ISO, with support of the ITA/IT Team, will implement and monitor audit controls both in Company ISP and Standard Operating Procedures and in Customer-facing Company Services.

### ***Preventative Controls***

Preventative controls are designed to discourage errors or irregularities from occurring in Company Services. Examples:

- Granular Company Service roles that can be assigned to individuals with Service access that prevent untrained individuals from:
  - Accessing unauthorized data
  - Creating new data
  - Editing/deleting existing data
  - Importing data
  - Exporting data
  - Changing system configurations
- Automated data input validation.
- User interface warning messages in workflows that result in new, changed, or deleted data.
- Configurable system business rules that allow different Customers to enforce different rules.
- Strict deletion rules and workflows that protect assets in use from being deleted.



### ***Detective Controls***

Detective controls are designed to find errors or irregularities after they have occurred. Examples:

- Integrated system feed completion and failure notifications.
- Integrated system data comparison.
- Large data deletion notifications.
- Data grid export to Excel for examination.

### ***Directive Controls***

Directive controls are designed to encourage a desirable outcome or behavior. Examples:

- SchoolFront and RecruitFront Knowledge Base articles (internal- and external-facing).
- Workflow Training (internal and external).
- Penalties associated with the restoration of compromised data from backup.

### ***Internal Company Auditing***

The ISO will also define procedures for routine internal auditing (where practical and beneficial) as well as procedures for responding to external audits and assisting Customers with audits as required.

## **Integrity**

The ISO, with support of the ITA/IT Team, will ensure that systems and applications managing Company Assets, Customer Assets, and PI have the capability to maintain data integrity at all times.

### ***Data Storage, Retention and Restoration of “Lost” Data***

See [Device and Media Controls](#).

### ***Source of Record Rules***

Where practical and beneficial, Source of Record rules are enforced to ensure that all new data and changes to groups of data originate from single sources. For example, in some integrations, a Company Service like SchoolFront, may receive feeds of data from another information system which can then be accessed and used within the Company Service for other tasks. If Source of Record rules are enforced, the imported information cannot be changed or updated in the Company Service. If new information, updates, changes, or deletions are required, all must be done in the Source information system.



## Person or Entity Authentication and Authorization

The ISO, with support of the ITA/IT Team, will implement and maintain controls that verify that a person seeking access to Company Assets, Customer Assets, and/or PI is the one claimed and enforce Company [password policy](#).

See also [Workforce Security](#).

## Transmission Security

The ISO, with support of the ITA/IT Team, will implement and maintain controls ensure that the integrity of Company Assets, Customer Assets, and PI is maintained when in transit. Secure transmission mechanisms that encrypt Company Assets, Customer Assets, and PI as well as confirms that data integrity has been maintained must be used.

See [Device and Media Controls](#).

The use of e-mail for transmitting Company Assets, Customer Assets, and/or PI should be avoided; if required, e-mails with Company Assets, Customer Assets, and/or PI should be encrypted.

## *Data and Media Transport*

Controls shall be in place to protect electronic and physical media containing Company data / information while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. “Electronic media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination is only authorized if the receiving party is an Authorized Recipient of such information, authorized by the Company’s ISO.

Company employees shall:

1. Protect and control electronic and physical media during transport.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.
3. Company employees will control, protect, and secure electronic and physical media during transport from public disclosure by:
  - a. Use of privacy statements in electronic and paper documents.
  - b. Limiting the collection, disclosure, sharing and use of Company data/information.
  - c. Following the least-privilege and role-based rules for allowing access. Limit access to Company data/information to only those people or roles that require access.

- d. Securing hand carried confidential electronic and paper documents by:
  - i. Storing Company data/information in a locked briefcase or lockbox.
  - ii. Only viewing or accessing the Company data/information electronically or document printouts in a physically secure location by authorized personnel.
  - iii. For hard copy printouts or Company documents:
    - 1. Package hard copy printouts in such a way as to not have any Company data/information viewable.
    - 2. That are mailed or shipped, receiving party must document procedures and only release to authorized individuals. **DO NOT MARK THE PACKAGE TO BE MAILED “CONFIDENTIAL.”** Packages containing data/information material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.  
(Receiving Party Discretion)
- e. Not taking Company data/information home or when traveling unless authorized by Company ISO.
- f. Disposing of confidential documents using a cross-cut shredder.
- g. Encryption.
- h. Following [best practices for domestic and foreign travel](#) with Company Assets and/or PI.