



**monroe one**  
EDUCATIONAL SERVICES

**Daniel T. White**  
*District Superintendent*

**Lisa N. Ryan**  
*Assistant Superintendent for Finance & Operations*

TO: Members of the Board of Education  
Mr. Daniel White

FROM: Lisa N. Ryan 

SUBJECT: Contract Approvals

DATE: July 5, 2023

The purpose of this memo is to request that at our July 13, 2023, Board of Education meeting the Board adopt a resolution to approve the following contracts:

- YouScience – Regional Information Center – per attached
- FrontEdge - Regional Information Center – per attached
- Panorama Education - District Office - per attached
- Humane Society of Rochester and Monroe County for the Prevention of Cruelty to Animals – Eastern Monroe Career Center – per attached
- Friendly Home - Eastern Monroe Career Center – per attached
- YMCA of Greater Rochester – Transition Department – per attached

Should you have any questions please contact me prior to our July 13 meeting. Thank you.



## FrontEdge AND MONROE 1 BOCES

### AGREEMENT

**AGREEMENT** made as of May 4, 2023 by, between, and among FrontEdge, Inc., having its offices at 274 North Goodman Street Suite B265, Rochester, NY, 14607 hereinafter referred to as "FrontEdge"), and The Monroe One Educational Services 41 O'Connor Road, Fairport, New York, 14450 (hereinafter referred to as "Monroe 1 BOCES"). FrontEdge enters this Agreement as an independent contractor and will remain as an independent contractor throughout the term of this agreement. FrontEdge employees shall not be entitled to any rights, payments or benefits afforded to the employees of Monroe 1 BOCES or participating school districts.

**1. Scope.** FrontEdge and Monroe 1 BOCES enter into affiliation solely for the purpose of offering school districts FrontEdge's modular web-based information management suite developed by FrontEdge. Through the affiliation, BOCES and/or participating school districts will be able to select services that they receive based on their individual/respective needs. FrontEdge will provide ongoing support and assistance to BOCES and/or participating school districts during the term of this Agreement.

**2. Terms and Termination.** This Agreement shall begin on July 1, 2023 and terminate on June 30, 2024; however, either of the parties may terminate this Agreement at any time and for any reason upon thirty (30) days' prior written notice to the other party. Participating school districts may elect to opt in or out of utilizing SchoolFront's product and/or services at any time during the term of this Agreement.

**3. Renewal.** The parties may renew this Agreement by written mutual agreement sixty (60) days' prior to the end of the term.

**4. Fees.** The fees for services selected by BOCES and/or participating school districts during the term of this Agreement are as follows:

SchoolFront EMS Pricing Sheet				
School/District Primary Contact Information				
Contact Name		Role		
Direct Phone Number				
Notes				
SchoolFront Pricing Fiscal year 23-24, each column has 1 user to identify the cost per user and represents "worst case scenario" as we provide multi-module discounts				
BOCES / District Name				
BOCES / District Address				
BOCES / District City		State		Postal Code
BOCES / District Main Phone Number				
Module / Service Pricing	Qty	One Time	Recurring	Recurring After Discount
SchoolFront Base	1	\$ 3,750.00	\$ 35.94	
Non-Teacher Evaluation Module (Rubrics Included)	1	\$ 1,100.00	\$ 20.29	
APPR Evaluation Module	1	\$ 1,750.00	\$ 23.19	
Personnel Folder Module	1	\$ 2,100.00	\$ 30.14	
Salary Adjustment Module	1	\$ 3,200.00	\$ 23.19	
Benefits Online Enrollment Module	1	\$ 1,200.00	\$ 13.91	
Professional Development Module	1	\$ 1,500.00	\$ 13.91	
Digital Form Module	1	\$ 1,200.00	\$ 5,796.37	
Employee Recruiting & Applicant Tracking Module	1	\$ 1,800.00	\$ 5,796.37	
Attendance	1	\$ 2,000.00	\$ 13.91	
Technology Integrations	1	\$ 250.00	\$ 579.64	
Scanning (Pulled from Scanning Services Worksheet)	1	\$ 0.27	\$ -	\$ -
<b>Attendance &amp; Safety Hardware (Does not include costs of running power and network drops)</b>				
Badges	0	\$ -	\$ -	\$ -
Battery Sensors	0	\$ -	\$ -	\$ -
Wired Only Sensors	0	\$ -	\$ -	\$ -
<b>Professional Services - Optional (Services requested beyond basic configuration and standard training)</b>				
Professional Services (Days)	1	\$ 1,500.00		
<b>Totals</b>				
Subtotal				
Multi-Module Discount				
After Multi-Module Discounts				
Additional Discount				
Proration Months				
BOCES Aidable Total After Discounts				
<b>Total Year 1 Costs (One-Time + Recurring)</b>				

Note: Professional services and scanning are estimates and actuals are billed.

BOCES and/or participating school districts will be invoiced for the services selected. In the event of early termination of services by a participating school district, FrontEdge will reimburse the fees to BOCES and/or the participating school district on a *pro rata* monthly basis.

**5. Indemnification.** Each party agrees to indemnify and hold each other and each of their officers, directors, employees agents and assigns, harmless from and against all claims, causes of action, damages, liabilities, fines, costs and expenses (including reasonable attorneys' fees) that may arise from the violation of the terms of this Agreement, violation of any applicable laws, infringement of third party proprietary and/or intellectual property rights, libel, slander and other torts including with respect to personal injury, property damage and death arising from the negligent or willfully wrongful acts or omissions of its employees, third-party vendors, contractors, subcontractors or agents, in connection with the services provided in connection with this Agreement.

**6. Cooperation.** The parties agree to cooperate with each other in connection with any internal investigations by FrontEdge or Monroe 1 BOCES of possible violation of their respective policies and procedures and any third party litigation.

**7. Confidentiality.** FrontEdge agrees that any and all data obtained from Monroe 1 BOCES and/or a participating school district shall be used expressly and solely for the purposes enumerated in this Agreement. Monroe 1 BOCES data and participating school district data shall not be distributed, used, or shared for any other purpose. FrontEdge shall not sell, transfer, share or process any Monroe 1 BOCES data or participating school district data for any purpose other than those under this Agreement, including commercial advertising, marketing, or any other commercial purpose. FrontEdge will comply with the terms and conditions set forth in the Education Law Section 2-d Contract Addendum, which is attached hereto as **Appendix A** and is incorporated by reference as if fully set forth herein. FrontEdge shall comply with all applicable laws, rules and regulations, including, but not limited to the Family Educational Rights and Privacy Act and New York Education Law Section 2-d and its implementing regulations.

**8. Independent Contractor:** This Agreement does not create an employee/employer relationship between the parties or between FrontEdge and any participating school district. FrontEdge will be an independent contractor and not a Monroe 1 BOCES or school district employee for any purpose whatsoever. No FrontEdge employee shall be entitled to any payment or benefit from Monroe 1 BOCES or a participating school district.

**9. Non-Discrimination and Legal Compliance.** FrontEdge agrees that it will not discriminate against anyone with respect to the provision of services hereunder on the grounds of race, religion, creed, color, national origin, gender, sexual orientation, disability, marital status, veteran status or other protected category. In providing the services pursuant to this Agreement, FrontEdge will comply with all applicable laws, rules and regulations.

**11. Jurisdiction.** This Agreement shall be governed by the laws of the State of New York. Litigation of all disputes between the parties arising from or in connection with this Agreement shall be conducted in a court of appropriate jurisdiction in the State of New York, County of Monroe, New York.

**12. Insurance.** Each party hereby agrees to obtain and thereafter maintain in full force and effect during the term of this Agreement general liability insurance with limits not less than \$1,000,000 per occurrence and \$2,000,000 annual aggregate.

13. **Order of Interpretation and Control.** In the event of a conflict between this Agreement, the Education Law Section 2-d Contract Addendum (Appendix A), or any other document, the Education Law Section 2-d Contract Addendum (Appendix A) shall control, and then this Agreement. FrontEdge shall not include any term in any such form or format that contradicts the terms to which it has agreed in this Agreement or with Education Law Section 2-d.

14. **Notices.** All notices to FrontEdge and Monroe 1 BOCES in connection with this Agreement shall be sent to:

Thomas Karafonda  
President, CEO  
FrontEdge, Inc.  
274 North Goodman Street Suite B265  
Rochester, NY 14607

All notices to Monroe 1 BOCES in connection with this Agreement shall be sent to:

Lisa N. Ryan  
Assistant Superintendent for Finance & Operations  
Monroe 1 BOCES  
41 O'Connor Road  
Fairport, NY 14450

15. **Entire Agreement.** This Agreement and Appendix A constitute the entire agreement between the parties.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first above written.

FrontEdge, Inc.

By: 

Thomas H. Karafonda

President, CEO

THE MONROE 1 BOARD OF COOPERATIVE  
EDUCATIONAL SERVICES

By: 

Daniel T. White

District Superintendent



**Appendix A**  
**Compliance With New York State Education Law Section 2-d Addendum ("Addendum")**

The parties to this Agreement are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and FrontEdge, Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Definitions

As used in this Agreement and related documents, the following terms shall have the following meanings: "Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student 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.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.

"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing;



(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U.S.);

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

(n) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Agreement.

**Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security**

<https://www.monroe.edu/domain/1478>

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320. (<https://www.monroe.edu/6320>)
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing, to:

Chief Privacy Officer  
New York State Education Department  
Room 863 EBA  
89 Washington Avenue  
Albany, New York 12234.

or

Monroe One Data Protection Officer  
William Gregory  
Monroe #1 BOCES  
41 O'Connor Road  
Fairport, NY 14450

**Supplemental Information About Agreement Between FrontEdge and BOCES**

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide FrontEdge's software and services to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.


(d) The effective date of this Agreement shall be July 1, 2023 and the Agreement shall remain in effect until June 30, 2024, unless sooner by either party for any reason upon thirty (30) days' notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vendor affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.

  
\_\_\_\_\_

Vendor Signature

\_\_\_\_\_ May 9, 2023



# ATTACHMENT 1 - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

## CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	By remaining in compliance with the SchoolFront Company Information Security Policy (ISP).
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Administrative: Assigned Security Responsibility, Risk Analysis, Risk Management, Acceptable Use, Activity Review, Workforce Security, Access Management, Communication/Awareness, Password Management, Incident Procedures, Monitoring & Routine Evaluation, Violations/ Sanctions. Physical: Environmental, Workstation, Device, and Media. Technical: Access Controls, Audit Controls, Integrity Controls, Authentication, Transmission Security
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Employees receive routine security refreshers, updates, and training related to the Company's ISP so that they remain aware of, and may remain in compliance with the information security and privacy policy and protection requirements.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Language about maintaining the security and privacy of customers / customer data is included in employment contracts signed by company employees upon hire.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized	All systems housing PII are professionally monitored to proactively identify vulnerabilities and/or incidents

	disclosures, and to meet your obligations to report incidents to the EA.	and incident reporting procedures are publicly posted on Company website. In the event of an incident, Contractor will promptly notify impacted customer(s) of any breach or unauthorized release of PII no later than seven (7) calendar days after discovery of a breach. Contractor will cooperate with the Customer(s) and law enforcement to protect the integrity of investigations regarding breach or unauthorized release of PII.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. Securely delete and destroy data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	EA PII accessible in production environment will be destroyed. Written certification provided upon request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor's privacy program/practices meet or exceed the requirements detailed in the EA's Data Privacy Agreement (which the Contractor also signed).
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

### ATTACHMENT 1(A) – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	<p><b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.</p>	<p>Physical devices and systems within the organization are inventoried. Software platforms and applications within the organization are inventoried. Organizational communication and data flows are mapped. External information systems are catalogued. Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customer, partners) are established.</p>
	<p><b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>The organization's role in the supply chain is identified and communicated. The organization's place in critical infrastructure and its industry sector is identified and communicated. Priorities for organizational mission, objectives, and activities are established and communicated.</p>
	<p><b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</p>	<p>Organizational cybersecurity policy is established and communicated. Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. Governance and risk management processes address cybersecurity risks.</p>
	<p><b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>Asset vulnerabilities are identified and documented. Cyber threat intelligence is received from information sharing forums and sources. Threats, both internal and external, are identified and documented. Potential business impacts and likelihoods are identified. Risk responses are identified and prioritized.</p>
	<p><b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>Risk management processes are established, managed, and agreed to by organizational stakeholders. Organizational risk tolerance is determined and clearly expressed. The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.</p>
	<p><b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>	<p>Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. Response and recovery planning and testing are conducted with suppliers and third-party providers.</p>

Function	Category	Contractor Response
PROTECT (PR)	<p><b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. Physical access to assets is managed and protected. Remote access is managed. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. Network integrity is protected (e.g., network segregation, network segmentation). Identities are proofed and bound to credentials and asserted in interactions. Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).</p>
	<p><b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>All users are informed and trained. Privileged users understand their roles and responsibilities. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities if applicable. Senior executives understand their roles and responsibilities. Physical and cybersecurity personnel understand their roles and responsibilities.</p>
	<p><b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>Data-at-rest is protected. Data-in-transit is protected. Assets are formally managed throughout removal, transfers, and disposition. Adequate capacity to ensure availability is maintained. Protections against data leaks are implemented. Integrity checking mechanisms are used to verify software, firmware, and information integrity. The development and testing environment(s) are separate from the production environment. Integrity checking mechanisms are used to verify hardware integrity</p>
	<p><b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality). A System Development Life Cycle to manage systems is implemented. Configuration change control processes are in place. Backups of information are conducted, maintained, and tested. Policy and regulations regarding the physical operating environment for organizational assets are met. Data is destroyed according to policy. Protection processes are improved. Effectiveness of protection technologies is shared. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. Response and recovery plans are tested. Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). A vulnerability management plan is developed and implemented.</p>
	<p><b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.</p>



Function	Category	Contractor Response
	<p><b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. Removable media is protected and its use restricted according to policy. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. Communications and control networks are protected. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.</p>
<p><b>DETECT (DE)</b></p>	<p><b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.</p>	<p>A baseline of network operations and expected data flows for users and systems is established and managed. Detected events are analyzed to understand attack targets and methods. Event data are collected and correlated from multiple sources and sensors. Impact of events is determined. Incident alert thresholds are established.</p>
	<p><b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>The network is monitored to detect potential cybersecurity events. The physical environment is monitored to detect potential cybersecurity events. Personnel activity is monitored to detect potential cybersecurity events. Malicious code is detected. Unauthorized mobile code is detected. External service provider activity is monitored to detect potential cybersecurity events. Monitoring for unauthorized personnel, connections, devices, and software is performed. Vulnerability scans are performed.</p>
	<p><b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p>Roles and responsibilities for detection are well defined to ensure accountability. Detection activities comply with all applicable requirements. Detection processes are tested. Event detection information is communicated. Detection processes are continuously improved.</p>
<p><b>RESPOND (RS)</b></p>	<p><b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>Response plan is executed during or after an incident.</p>
	<p><b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>Personnel know their roles and order of operations when a response is needed. Incidents are reported consistent with established criteria. Information is shared consistent with response plans. Coordination with stakeholders occurs consistent with response plans. Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.</p>
	<p><b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>Notifications from detection systems are investigated. The impact of the incident is understood. Forensics are performed. Incidents are categorized consistent with response plans. Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).</p>

Function	Category	Contractor Response
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incidents are contained. Incidents are mitigated. Newly identified vulnerabilities are mitigated or documented as accepted risks.
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response plans incorporate lessons learned. Response strategies are updated.
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Recovery plan is executed during or after a cybersecurity incident.
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned. Recovery strategies are updated.
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Public relations are managed. Reputation is repaired after an incident. Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

## 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](https://RecruitFront.com),
- [Support.RecruitFront.com](https://Support.RecruitFront.com),
- [App.RecruitFront.com](https://App.RecruitFront.com), and
- [X.recruitfront.com](https://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.