

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 [COMPANY], 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 [COMPANY] 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 Incident IQ's Platform 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.

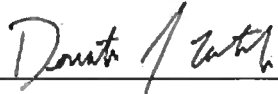
(d) The effective date of this Agreement shall be [DATE] and the Agreement shall remain in effect until June 30, 2025, unless sooner by either party for any reason upon thirty (30) days' notice.

(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 vender 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

_____ June 12 _____, 2024

TIPS 220105 Technology Solutions, Products and Services		Incident IQ, LLC				
EQUIPMENT/GOODS by line	Product #	Description	Units description - (each, dozen, hour, day, etc)	MSRP	% Discount	TIPS Price
IIQ PLATFORM with TICKETING	IIQ-1000	The underlying platform that powers Incident IQ. When selected with Ticketing, the Platform includes the Help desk solution that K-12 districts use to easily and intelligently manage help requests. Additional add-ons listed below.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$5/s and no less than \$1.75/s; For Districts 10000-39999 students, no more than \$3.50/s and no less than \$1.40/s; For Districts 40000-74999 students, no more than \$2.50/s and no less than \$1/s. For Districts 75000+, no more than \$2/s, no less than \$1/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for Inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
IIQ PLATFORM with ASSETS	IIQ-2000	The underlying platform that powers Incident IQ. When selected with Assets, the Platform provides Enterprise-level asset management tools, built for the scale of today's K-12 technology. Deployment, collection, management, auditing—IIQ Assets supports the technology that's transforming today's classrooms. Assets includes other functionalities. Additional add-ons listed below	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$5/s and no less than \$1.75/s; For Districts 10000-39999 students, no more than \$3.50/s and no less than \$1.40/s; For Districts 40000-74999 students, no more than \$2.50/s and no less than \$1/s. For Districts 75000+, no more than \$2/s, no less than \$1/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for Inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
IIQ PLATFORM with FACILITIES	IIQ-3000	The underlying platform that powers Incident IQ. When selected with Facilities the Platform includes modern facilities management software, built for K-12 school districts. Additional add-ons listed below	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$5/s and no less than \$1.75/s; For Districts 10000-39999 students, no more than \$3.50/s and no less than \$1.40/s; For Districts 40000-74999 students, no more than \$2.50/s and no less than \$1/s. For Districts 75000+, no more than \$2/s, no less than \$1/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for Inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADD-ON: IIQ TICKETING	IIQ-6100	When ordered as an add-on to IIQ Platform w/ ASSETS or W/ FACILITIES: Help desk solution that K-12 districts use to easily and intelligently manage help requests	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$3/s and no less than \$1.50/s; For Districts 10000-39999 students, no more than \$2.50/s and no less than \$1/s; For Districts 40000-74999 students, no more than \$2/s and no less than \$0.75/s. For Districts 75000+, no more than \$1.75/s, no less than \$0.50/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for Inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis

ADD-ON: IIQ ASSETS	IIQ-6200	When ordered as an add-on to IIQ Platform w/ TICKETING or FACILITIES: Enterprise-level asset management tools, built for the scale of today's K-12 technology. Deployment, collection, management, auditing—IIQ Assets supports the technology that's transforming today's classrooms.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$3/s and no less than \$1.50/s; For Districts 10000-39999 students, no more than \$2.50/s and no less than \$1/s; For Districts 40000-74999 students, no more than \$2/s and no less than \$0.75/s. For Districts 75000+, no more than \$1.75/s, no less than \$0.50/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADD-ON: FACILITIES	IIQ-6300	When ordered as an add-on to IIQ Platform w/ ASSETS or TICKETING: Modern facilities management software, built for K-12 school districts.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$3/s and no less than \$1.50/s; For Districts 10000-39999 students, no more than \$2.50/s and no less than \$1/s; For Districts 40000-74999 students, no more than \$2/s and no less than \$0.75/s. For Districts 75000+, no more than \$1.75/s, no less than \$0.50/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADD-ON: POLICY MANAGER	IIQ-8100	Create, distribute, and manage student and employee policies with Policy Manager. Deliver policy agreements and forms through multiple portals—through Incident IQ, a direct URL, or through student ID lookup. Segment audiences by location, role, or through individual student or staff lists. Policy Manager makes it simple to create a trusted channel to quickly distribute district agreements.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$1/s and no less than \$0.50/s; For Districts 10000-39999 students, no more than \$0.75/s and no less than \$0.30/s; For Districts 40000-74999 students, no more than \$0.68/s and no less than \$0.22/s. For Districts 75000+, no more than \$0.25/s, no less than \$0.15/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADD-ON: PASSWORD ASSISTANT	IIQ-8200	Streamline password resets and recovery for all major SSO environments including Google SSO, Microsoft Azure and ADFS with Password Assistant	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$1/s and no less than \$0.50/s; For Districts 10000-39999 students, no more than \$0.75/s and no less than \$0.30/s; For Districts 40000-74999 students, no more than \$0.68/s and no less than \$0.22/s. For Districts 75000+, no more than \$0.25/s, no less than \$0.15/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis

ADD-ON: SUPPORT SCHEDULER	IIQ-8300	Get support sessions booked with ease. Give requestors your available windows, and have them select the time that works best.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$1/s and no less than \$0.50/s; For Districts 10000-39999 students, no more than \$0.75/s and no less than \$0.30/s; For Districts 40000-74999 students, no more than \$0.68/s and no less than \$0.22/s. For Districts 75000+, no more than \$0.25/s, no less than \$0.15/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for Inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADD-ON: SUPPORT MESSENGER	IIQ-8400	Support Messenger is a real time communication app for Incident IQ. Send direct messages, start group chats, drag and drop files, and get help requests solved even faster.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$1/s and no less than \$0.50/s; For Districts 10000-39999 students, no more than \$0.75/s and no less than \$0.30/s; For Districts 40000-74999 students, no more than \$0.68/s and no less than \$0.22/s. For Districts 75000+, no more than \$0.25/s, no less than \$0.15/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for Inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADD-ON: FORMS MANAGER	IIQ-850X	Build, manage, and distribute custom forms to collect data within your Incident IQ workflows. Digitize stacks of cluttered paperwork and keep it organized and accounted for.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$0.50/s and no less than \$0.40/s; For Districts 10000-39999 students, no more than \$0.39/s and no less than \$0.30/s; For Districts 40000-74999 students, no more than \$0.29/s and no less than \$0.20/s. For Districts 75000+, no more than \$0.20/s, no less than \$0.14/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for Inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADDON- Payment Integration	IIQ-8510 (Intouch) IIQ-8520 (Stripe) IIQ-8530 (Square) IIQ-8540 (MySchoolBucks) IIQ-8550 (Vanco)	integrations for payment integration allows K-12 districts to attach payments to help tickets, users, and assets. This integrations ensure seamless and secure data communication between Incident IQ and integrating platform	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$1/s and no less than \$0.50/s; For Districts 10000-39999 students, no more than \$0.75/s and no less than \$0.30/s; For Districts 40000-74999 students, no more than \$0.68/s and no less than \$0.22/s. For Districts 75000+, no more than \$0.25/s, no less than \$0.15/s			

ADD-ON: Enhanced Approval Workflow	IIQ-8600	The Enhanced Approval Workflows app empowers districts with new tools to better manage specific workflows that require one or more approvals. Maintain district compliance requirements, keep records on past approvals, and make informed decisions.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$3/s and no less than \$1.50/s; For Districts 10000-39999 students, no more than \$2.50/s and no less than \$1/s; For Districts 40000-74999 students, no more than \$2/s and no less than \$0.75/s. For Districts 75000+, no more than \$1.75/s, no less than \$0.50/s			
ADD-ON: HR Service Delivery	IIQ-6500	Keep onboarding processes organized and optimized. Assign onboarding tasks automatically, track progress, and get visibility over every new hire in your district.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$3/s and no less than \$1.50/s; For Districts 10000-39999 students, no more than \$2.50/s and no less than \$1/s; For Districts 40000-74999 students, no more than \$2/s and no less than \$0.75/s. For Districts 75000+, no more than \$1.75/s, no less than \$0.50/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADD-ON: Events	IIQ-6600	iiQ Events provides tools to handle customizable room reservations, along with coordinating preparation for an event. Manage reservations, approvals, and preparation tasks, with a solution designed for K-12 educational institutions; Only available when ordered as an add-on to IIQ Platform w/ FACILITIES.	per district, priced using a proprietary pricing model analyzing per student enrolled basis w/in ranges; For Districts 1000 - 9999 students, no more than \$3/s and no less than \$1.50/s; For Districts 10000-39999 students, no more than \$2.50/s and no less than \$1/s; For Districts 40000-74999 students, no more than \$2/s and no less than \$0.75/s. For Districts 75000+, no more than \$1.75/s, no less than \$0.50/s	Catalog pricing to be provided upon request (https://www.incidentiq.com/pricing)	2.50%	TIPS price for inquiring members will be calculated applying 2.5% discount to what would have been the per district price after using the Incident IQ proprietary pricing model analyzing per student enrolled basis
ADDL ITEMS TO BE UPDATED AS RELEASED						

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.	See attached Incident IQ Data Privacy & Security Plan
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See attached Incident IQ Data Privacy & Security Plan
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.	See attached Incident IQ Data Privacy & Security Plan
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.	See attached Incident IQ Data Privacy & Security Plan
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 disclosures, and to meet your obligations to report incidents to the EA.	See attached Incident IQ Data Privacy & Security Plan
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See attached Incident IQ Data Privacy & Security Plan
7	Describe your secure destruction practices and how certification will be provided to the EA.	See attached Incident IQ Data Privacy & Security Plan
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See attached Incident IQ Data Privacy & Security Plan
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)	Asset Management (ID.AM): 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.	See attached Incident IQ Data Privacy & Security Plan
	Business Environment (ID.BE): 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.	See attached Incident IQ Data Privacy & Security Plan
	Governance (ID.GV): 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.	See attached Incident IQ Data Privacy & Security Plan
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	See attached Incident IQ Data Privacy & Security Plan
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	See attached Incident IQ Data Privacy & Security Plan
	Supply Chain Risk Management (ID.SC): 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	See attached Incident IQ Data Privacy & Security Plan

Function	Category	Contractor Response
PROTECT (PR)	processes to identify, assess and manage supply chain risks.	See attached Incident IQ Data Privacy & Security Plan
	Identity Management, Authentication and Access Control (PR.AC): 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.	See attached Incident IQ Data Privacy & Security Plan
	Awareness and Training (PR.AT): 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.	See attached Incident IQ Data Privacy & Security Plan
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	See attached Incident IQ Data Privacy & Security Plan
	Information Protection Processes and Procedures (PR.IP): 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.	See attached Incident IQ Data Privacy & Security Plan
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	See attached Incident IQ Data Privacy & Security Plan
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	See attached Incident IQ Data Privacy & Security Plan
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	See attached Incident IQ Data Privacy & Security Plan
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	See attached Incident IQ Data Privacy & Security Plan
	Detection Processes (DE.DP): Detection processes and procedures are maintained	See attached Incident IQ Data Privacy & Security Plan

Function	Category	Contractor Response
	and tested to ensure awareness of anomalous events.	See attached Incident IQ Data Privacy & Security Plan
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	See attached Incident IQ Data Privacy & Security Plan
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	See attached Incident IQ Data Privacy & Security Plan
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	See attached Incident IQ Data Privacy & Security Plan
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	See attached Incident IQ Data Privacy & Security Plan
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	See attached Incident IQ Data Privacy & Security Plan
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	See attached Incident IQ Data Privacy & Security Plan
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	See attached Incident IQ Data Privacy & Security Plan
	Communications (RC.CO): 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).	See attached Incident IQ Data Privacy & Security Plan

Incident IQ
DATA PRIVACY AND SECURITY PLAN

Incident IQ, LLC (“Incident IQ, We, Us, or Our”), as a covered third-party contractor under NYS Education Law 2-d shall undertake all of the following data privacy, security, and protection measures, in addition to the requirements already contained in the Incident IQ Cloud Services Master Subscription Agreement (available at <https://www.incidentiq.com/legal>):

1. Data Collection & Use:

- a. Incident IQ shall only collect, process and store such Protected Data to which we have a legitimate educational interest and as is necessary to provide the cloud services.
- b. Under no circumstances will Incident IQ use Protected Data to market or advertise to students or their family members or legal guardians, or otherwise use Protected Data to inform, influence or enable marketing, advertising or other commercial efforts by a third party directed at students, their family members, or legal guardians.
- c. We shall not change how Protected Data are collected, maintained, used or disclosed under the terms of the Agreement, without advance notice to and prior written consent from District.
- d. We will never sell Protected Data that we acquire through District use of the Cloud Services, except as part of a corporate purchase, merger or other type of acquisition. In such a case, any successor entity shall be contractually obligated to comply with the terms of this Agreement related to the treatment of Protected Data, as well as all other applicable legal requirements governing the use, disclosure, and security of the previously acquired Protected Data.

2. Data Portability: Incident IQ shall ensure the data portability of all District data.

- a. Upon notice of a request from District for a copy of certain Protected Data in Our possession (e.g., to support the District’s response to a properly constituted request for Protected Data from a parent, guardian or student), we will ensure that: (i) A complete and readable digital copy of the requested Protected Data in Incident IQ’s possession is delivered to District within 30 days of our receipt of District’s request; (ii) Upon delivery of the copy, District must provide notice to Incident IQ of District’s receipt and acceptance of any such requested Protected Data;
- b. Upon notice of a request from District that certain Protected Data be deleted, We will permanently destroy (i.e., undertake a non-recoverable deletion process in accordance with Department of Defense standard 5220.22-M) all copies of the Protected Data identified for deletion by District held by Us or any of Our agents, subcontractors or affiliates. Within 30 days of District notice, we will deliver a written confirmation to District certifying that the permanent destruction of the requested Protected Data has been accomplished. Upon delivery of such written confirmation of deletion, District must provide notice to Us of District receipt and understanding of said notice confirming deletion made at District request.
- c. We shall destroy all Protected Data residing in District’s instance of the Cloud Services, using the methods described in paragraph 2(b) above, following expiration of a 60-day period after termination of this Agreement, unless District requests that We return such information to District instead.

3. Data Security:

- a. We will operate the Cloud Services and collect, process and store Protected Data in accordance with NIST data security standards and current industry best practices, and maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of Protected Data, and prevent unauthorized access, disclosure and use.
- b. All information is stored within databases hosted and secured within the Microsoft Azure Cloud. The Azure cloud is secured with actively monitored network firewalls, intrusion detection systems, application firewalls, and IP-route protection. Additionally, any information designated as Protected Data is encrypted within the database.
- c. No data shall be stored outside the United States; all data are stored in the Microsoft Azure data center, region East US (Virginia), East US 2 (Virginia), and/or West US (California).
- d. Any data designated as Protected Data which include passwords, is encrypted within the database using combinations of one-way and two-way encryption algorithms (such as SHA256) with Salt strings.
- e. Information is multi-tenanted and stored within the same cloud systems; however, all information is partitioned by a School District ID (i.e., SiteId) and the Data Access Layers forces all data to be filtered by a specific School District.
- f. Physical servers are physically secured in the Microsoft Azure data centers, regions East US (Virginia), East US 2 (Virginia), and West US (California).
- g. Data in transit are SSL protected, as well as Protected Data are always encrypted.
- h. Only Incident IQ Senior Technical Team members have direct access to product data. All personnel with access to Incident IQ systems and data are vetted via backgrounds checks and receive annual and update training on all relevant policies and procedures.
- i. No software functions are subcontracted to other vendors apart from the hosting/storage services provided by Microsoft, as described above.
- j. Customer support representatives accordingly confirm caller identity against a District's list of administrator-users. Account creation and deletion is controlled by the District as user profiles are established through syncing with the client's identity management provider (e.g., Microsoft ADFS, Google SSO, local Active Directory, etc.). Accordingly, account creation/deletion is managed by the District through their ordinary identity management policies and procedures. Also, permissions modification of any given user may be managed by the clients' administrator-level users through tools in their admin console. If assistance were required in this process admin-users would authenticate with customer support representatives as described above.

4. Network Operations Center Management and Security:

- a. Incident IQ shall perform regular penetration testing, vulnerability management and intrusion prevention testing.
- b. All network devices shall be located in secure facilities under controlled circumstances (i.e., ID cards and entry logs) at the Microsoft Azure data centers, regions East US (Virginia), East US 2 (Virginia), and West (California).
- c. Backups shall be performed daily (to other US-based Azure Data Centers), as well as backups made to separate secure, off-site facility.
- d. Backups shall be encrypted and stored securely with access limited to administrators with restoration encryption keys.
- e. All software vulnerabilities shall be patched routinely or automatically in accordance with the following parameters: all critical and High vulnerabilities shall be patched automatically. Medium vulnerabilities shall be patched monthly during planned maintenance windows. Low vulnerabilities shall be evaluated and if deemed necessary, shall be patched during the planned monthly maintenance window.
- f. Incident IQ shall respond to any incidents IAW its Incident Response Plan.