EDUCATION LAW 2-D PROJECT MANAGEMENT TOOL

Use the chart below to identify a potential educational agency timeline for completing the Education Law 2-d requirements. While all of the requirements impact educational agencies' daily practice, shading is used to highlight areas that require formal ongoing work and maintenance.

CATEGORIES	TASK	REG	PAGES	TIMELINE	COMPLETE
PROTECTION OF PII	Guidelines for Personally Identifiable Information Utilization Defined and Communicated to all Staff	121.2 121.5 121.7	5		☐
BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY	Parents' Bill of Rights Published on District Website	121.3	6 - 9		☐
	Supplemental Information Related to Third-Party Contracts Published on District Website				☐
DATA SECURITY AND PRIVACY POLICY	Data Security and Privacy Policy Adopted and Notice Provided to Staff and Officers	121.5	10	By Oct. 1, 2020	☐
NIST CYBERSECURITY FRAMEWORK	NIST CSF Aligned 2019-2020 Current Profile Developed	121.5	11 - 12		☐
	NIST CSF Aligned Security and Privacy Plan (Profile and Action Plan) Developed and Maintained				☐
THIRD-PARTY CONTRACTS	Inventory of Third-Party Contracts Developed and Maintained	121.2 121.3 121.6 121.9 121.10	13 - 14 Appendix		☐
	Compliant Terms and Conditions Negotiated into Contracts (or Separate Data Sharing and Confidentiality Agreements) with Third-Party Contractors, Where Necessary				☐
ANNUAL EMPLOYEE TRAINING	Employee Training Implemented	121.7	15		☐
UNAUTHORIZED DISCLOSURE COMPLAINT PROCEDURES	Complaint Procedures Defined	121.4	16 -17		☐
	Breach, Unauthorized Release, and Complaint Record Maintained				☐
INCIDENT REPORTING AND NOTIFICATION	Incident Reporting and Notification Procedures and Resources Developed	121.10	18 - 19		☐
DATA PROTECTION OFFICER	Data Protection Officer Designated or Appointed	121.8	20 - 21		☐

NYS REQUIREMENTS FOR DATA SECURITY AND PRIVACY

Education Law 2-d and Part 121 of the Commissioner's Regulations outline requirements for school districts and BOCES related to the protection of the personally identifiable information (PII) of students, as well as some teacher and principal information. The law and the regulations require schools to undertake a multi-pronged approach to information governance.

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Protect the confidentiality of student PII (as defined in FERPA) and certain teacher and principal PII (confidential APPR data)

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Develop and post, on the agency's website, a Parents Bill of Rights with supplemental information about each agreement with a third-party contractor that involves disclosure of PII

DATA SECURITY AND PRIVACY POLICY

Adopt and post a Data Security and Privacy Policy that includes adherence to the NIST Cybersecurity Framework to protect PII

NIST CYBERSECURITY FRAMEWORK

Apply the planning, processes, and categories of information protection defined within the NIST Cybersecurity Framework to district practices

THIRD-PARTY CONTRACTS

Whenever a contractor receives protected PII, ensure that the agreement for using the product or services (or, an addendum to that agreement) includes required language

ANNUAL EMPLOYEE TRAINING

Deliver annual privacy and security awareness training to all employees with access to protected data

UNAUTHORIZED DISCLOSURE COMPLAINT PROCEDURES

Create and publish a complaint process

INCIDENT REPORTING AND NOTIFICATION

Follow reporting and notification procedures when a breach or unauthorized disclosure occurs

DATA PROTECTION OFFICER

Appoint a Data Protection Officer to oversee implementation of Education Law 2-d responsibilities

DATA PROTECTION OFFICER

Each educational agency must designate a Data Protection Officer (DPO) to be responsible for the implementation of the policies and procedures required in Education Law 2-d. The designee will also serve as the point of contact for data security and privacy for the educational agency. To learn more about this requirement, agencies can review Part 121.8 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Data Protection Officer:

- ✓ Is Identified
- ✓ Has Clear Roles and Responsibilities

DPO REGULATORY RESPONSIBILITIES

IMPLEMENTATION OF ED LAW 2-D PROCEDURES
The DPO is responsible for the implementation of the policies and procedures required by Education Law 2-d.

DATA SECURITY AND PRIVACY LEADER
The DPO is the point of contact for data security and privacy for the educational agency.

ADDITIONAL REGULATORY GUIDELINES

KNOWLEDGE, TRAINING AND EXPERIENCE REQUIRED
The DPO must have the appropriate knowledge, training and experience to administer the functions.

EXISTING EMPLOYEE CAN PERFORM FUNCTIONS
A current employee of an educational agency may perform the DPO function in addition to other job responsibilities.

CONSIDERATIONS RELATED TO NIST

AWARENESS AND TRAINING CATEGORY
Personnel are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
Specifically:

- All users are informed and trained
- Privileged users understand their roles and responsibilities
- Senior executives understand their roles and responsibilities
- Physical and cybersecurity personnel understand their roles and responsibilities

MODEL DATA PROTECTION OFFICER JOB DESCRIPTION

In consultation with the superintendent the Data Protection Officer shall:

JOB RESPONSIBILITIES:

- Serve as the point of contact for data security and privacy for the educational agency.
- Implement privacy governance measures to manage the use of personally identifiable information to ensure compliance with Education Law 2-d.
- Coordinate the implementation of the policies and procedures required under Education Law 2-d and Part 121.
- Monitor the educational agency's compliance with state and federal data privacy laws and regulations.
- Develop an incident response plan and a procedure for stakeholders to file complaints about breaches or unauthorized releases of student data.
- Facilitate the delivery of an annual information privacy and security awareness training.
- Review projects, contracts and procurements that will create, collect or process personally identifiable information for compliance.
- Develop and maintain the educational agencies Data Security and Privacy Action Plan.

PREFERRED KNOWLEDGE, SKILLS AND ABILITIES:

- Must have appropriate knowledge, training and experience to implement the district's data security and privacy program, in compliance with Education Law 2-d.
- Ability to interact effectively with people at all organizational levels of the agency.
- Ability to exercise leadership, influence change and implement solutions.
- Ability to handle confidential and sensitive information with discretion.

ORGANIZATIONAL RELATIONSHIPS:

- Reporting structure provides access to leaders with decision making authority.
- Reports annually to the Board of Education on the agency's data security and privacy posture.
- Collaborates with stakeholders (IT, internal audit, school attorneys, etc.) to fulfill this role.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Education Law Section 2-d and Part 121 of the Commissioner's Regulations outline requirements for educational agencies and their third-party contractors to strengthen data privacy and security in order to protect student and annual professional performance review personally identifiable information.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Security and Privacy Plan:

- ✓ Defines Data Governance Structures
- ✓ Includes a Comprehensive Data and Systems Inventory

Ed Law 2-d Deliverables:

- ✓ Demonstrate Compliance with All Ed Law 2-d Requirements
  (Requirements are Explained on Subsequent Pages)

PROTECTED DATA

PROTECTED STUDENT DATA

The term "student" refers to any person attending or seeking to enroll in an educational agency, and the term "personally identifiable information" ("PII") uses the definition provided in FERPA. The term PII includes, but is not limited to:

- Student Name
- Parent Names
- Student ID Num
- Student Email
- Student Address
- Student Photos
- Video of Students
- Student Birthdate
- Student Medical Information
- Special Education Information
- Other indirect identifiers
- Information that, alone or in combination, would allow a reasonable person to identify the student

TEACHER AND PRINCIPAL DATA

Personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §3012-c and §3012-d is subject to Education Law 2-d.

ED LAW 2-D AND DIRECTORY INFORMATION

THIRD-PARTY CONTRACTORS

All FERPA "directory information" continues to be PII under Ed Law 2-d. As a result, agencies can not disclose PII that has been designated as directory information to third-party contractors without an Education Law 2-d compliant agreement.

NEWSLETTERS AND SOCIAL MEDIA

If a newsletter is composed and printed in-house or by a BOCES, there is no sharing with a contractor and Ed Law 2-d does not apply. Please note, FERPA would still apply. PII might be allowed in communications based on a "directory information" or "school official" analysis. If a newsletter is printed by an outside vendor, or, composed on and/or distributed over the Internet in such a manner that an outside vendor receives the student data, then Ed Law 2-d applies and a compliant third-party contract is needed.

DATA SECURITY AND PRIVACY POLICY

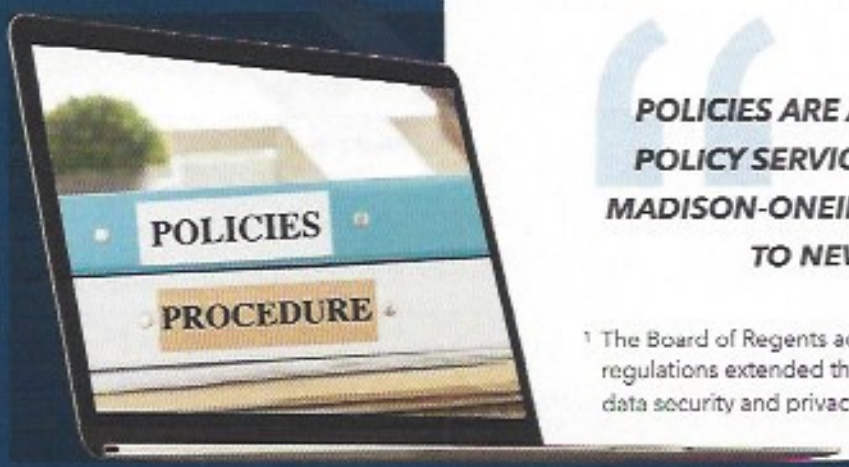
Part 121 of the Commissioner's Regulations requires agencies to adopt a policy on data security and privacy by October 1, 2020.[1] Additionally, the law requires agencies to publish the policy on the district's website. To learn more about this requirement, review Part 121.5 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Policy:

- ✓ Includes All Required Elements
- ✓ Is Adopted by October 1, 2020
- ✓ Is Posted on the Agency's Website
- ✓ Notice is Provided to All Officers and Employees
- ✓ Third-Party Contracts Require Practices Consistent with the Policy



REQUIRED ELEMENTS

NIST CYBERSECURITY FRAMEWORK ALIGNMENT
Policy must align with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF)

DATA GOVERNANCE
Every use and disclosure of PII by the educational agency must benefit students and the agency

DISCLOSURE AVOIDANCE
Personally identifiable information will not be included in public reports or other documents

PROTECTIONS AFFORDED TO PARENTS
Include all the protections afforded to parents or eligible students, where applicable, under FERPA and IDEA, and the federal regulations implementing such statutes

CONSISTENT WITH STATE AND FEDERAL LAWS
Consistent with applicable state and federal laws

POLICIES ARE AVAILABLE THROUGH DISTRICTS' POLICY SERVICES. NYSSBA, ERIE 1 BOCES, AND MADISON-ONEIDA BOCES OFFER POLICY SERVICES TO NEW YORK STATE DISTRICTS.

[1] The Board of Regents adopted emergency regulations on June 8, 2020. The regulations extended the date required for the adoption and publishing of data security and privacy policies from July 1, 2020 until October 1, 2020.

BILL OF RIGHTS

A Parents' Bill of Rights for Data Privacy and Security must be published on the website of each educational agency and must be included with every contract an educational agency enters into with a third-party contractor that receives personally identifiable information. The list below highlights required elements that must be included in the Parents' Bill of Rights. To learn more about this requirement, agencies can review Part 121.3 of the Regulations and Section 3 of Education Law 2-d.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Bill of Rights:

- ✓ Includes All Elements
- ✓ Is Posted on the District's Website
- ✓ Includes Supplemental Information for All Relevant Contracts
- ✓ Is Included and Signed in All Relevant Contracts

REQUIRED ELEMENTS

DATA WILL NOT BE SOLD
A student's personally identifiable information cannot be sold or released for any commercial purposes

THE RIGHT TO REVIEW CHILD'S RECORD
Parents have the right to inspect and review the complete contents of their child's education record

DATA IS PROTECTED
State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices must be in place when data is stored or transferred

NYSED COLLECTED DATA
A complete list of all student data elements collected by the State is available for public review. Districts must include an appropriate NYSED link and NYSED mailing address for parents.

BREACH COMPLAINT CONTACT
Parents have the right to have complaints about possible breaches of student data addressed. Districts must include appropriate complaint submission contact information (e.g. phone number, email and address).

SUPPLEMENTAL INFORMATION
Supplemental information for each contract an educational agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data.

MUST BE CLEAR AND IN PLAIN ENGLISH

MODEL PARENTS' BILL OF RIGHTS

DISTRICT seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the district, to enhance the opportunities for learning and to increase the efficiency of our operations. To assist in meeting 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, DISTRICT 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, No. [Insert Number].

(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.nysed.gov/data-privacy-security/student-data-inventory 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.

- Parents may make a written report of a possible breach of student data to the DISTRICT Data Protection Officer by email at [Insert e-mail address] or by regular mail at [insert address].
- Complaints may also be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 1223 or by submitting a form at: http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

We are compiling the following information about each agreement between DISTRICT and an outside party that receives protected student data, or protected principal or teacher data, from the district: (1) the exclusive purposes for which the data will be used, (2) how the contractor will ensure that any subcontractors it uses will abide by data protection and security requirements, (3) when the contract expires and what happens to the data at that time, (4) if and how an affected party can challenge the accuracy of the data, (5) where the data will be stored, and (6) the security protections taken to ensure the data will be protected, including whether the data will be encrypted. The links below will take you to that information for the listed agreements. We will be updating this list as we gather additional information.

BILL OF RIGHTS SUPPLEMENTAL INFORMATION

Educational agencies are required to post information about third-party contracts on the agency's website with the Bill of Rights. Supplemental information may be redacted to the extent necessary to safeguard the data. To learn more about this requirement, review Part 121.3 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Supplmental Information:

- ✓ Includes All Elements
- ✓ Is Posted on the District's Website
- ✓ Includes Supplemental Information for All Relevant Contracts
- ✓ Includes Links or Attachments to Relevant BOCES/RIC Contracts

REQUIRED ELEMENTS

The supplemental information must be developed by the educational agency and include the following information:

EXCLUSIVE PURPOSE FOR DATA USE
The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

SUBCONTRACTORS MANAGEMENT
How the contractor will ensure that the subcontractors, if any, will abide by all applicable data protection requirements, including but not limited to those outlined in applicable state and federal laws and regulations;

CONTRACT DURATION AND DATA DESTRUCTION
The duration of the contract, including the contract's expiration date and a description of what will happen to the data upon expiration of the contract or other written agreement;

DATA ACCURACY
If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

LOCATION OF THE DATA AND SECURITY PRACTICES
Where the data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated;

ENCRYPTION
Address how the data will be protected using encryption while in motion and at rest.

MAY BE REDACTED TO THE EXTENT NECESSARY TO SAFEGUARD THE AGENCY'S DATA AND/OR TECHNOLOGY INFRASTRUCTURE

MODEL SUPPLEMENTAL INFORMATION

The supplemental information must reflect the language of each specific data sharing agreement with a vendor. An example is provided below.

CONTRACTOR	[Vendor Name]
PRODUCT	[Product Name]
PURPOSE DETAILS	The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT. The product or services are used to provide [e.g., mathematics instruction in Grades 1 and 2].
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.
CONTRACT DURATION AND DATA DESTRUCTION INFORMATION	The agreement expires [Insert Date]. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT. Upon expiration of this Contract with a successor agreement in place, Vendor will cooperate with the DISTRICT as necessary to transition protected data to the successor vendor prior to deletion. Vendor shall thereafter securely delete and overwrite any and all Protected Information 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 of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
DATA ACCURACY INFORMATION	In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Education Rights and Privacy Act.
SECURITY PRACTICES INFORMATION	The data is stored in the continental United States (CONUS) or Canada. Vendor will maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).

SAMPLE DATA SHARING AND CONFIDENTIALITY AGREEMENT

EXHIBIT [__]
DATA SHARING AND CONFIDENTIALITY AGREEMENT
Including
[Name of District] Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
[Name of District] and [Name of Vendor]

1. **Purpose**
   (a) [Name of District] (hereinafter "District") and [Name of Vendor] (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the "Master Agreement").

   (b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between [Name of District] and [Name of Vendor] that the District is required by Section 2-d to post on its website.

   (c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**
   As used in this Exhibit:

   (a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

   (b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between [Name of District] and [Name of Vendor]." Vendor's obligations described within this section include, but are not limited to:

(i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and

(ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting [Name of District Contact] directly by email at [Email address] or by calling [Phone number].

(c) Vendor will cooperate with the District and provide as much information as possible directly to [Name of District Contact] or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform [Name of District Contact] or his/her designee.

SAMPLE DATA SHARING AND CONFIDENTIALITY AGREEMENT

6. **Additional Statutory and Regulatory Obligations[1]**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); i.e., they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy, Section 2-d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

SAMPLE DATA SHARING AND CONFIDENTIALITY AGREEMENT

EXHIBIT [__] (CONTINUED)
Bill of Rights for Data Security and Privacy
[Name of District]

[INSERT District's Bill of Rights for Data Security and Privacy here]

BY THE VENDOR:

_____
Name (Print)

_____
Signature

_____
Title

_____
Date

EXHIBIT [__] (CONTINUED)
Supplemental Information about a Master Agreement between
[Name of District] and [Name of Vendor][2]

[Name of District] has entered into a Master Agreement with [Name of Vendor], which governs the availability to the District of the following products or services:

[List specific product or services from Vendor here]

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

SAMPLE DATA SHARING AND CONFIDENTIALITY AGREEMENT

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreement commences on [Date] and expires on [Date].
- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

SAMPLE DATA SHARING AND CONFIDENTIALITY AGREEMENT

1 Nothing in Education Law Section 2-d or Part 121 specifically requires an educational agency to include within its contracts with third-party contractors this list of obligations that are imposed on third-party contractors by the statute and/or its implementing regulations. However, many school districts and other educational agencies have considered it a best practice to include these statutory and regulatory obligations within their third-party contracts.

2 Each educational agency, including a school district, is required to publish a "Bill of Rights for Data Security and Privacy" on its website. See, Education Law Section 2-d(3)(a) and Part 121.3(a). The Bill of Rights [that is posted on a district's website] must also include "supplemental information" for each contract that the school district enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data [protected by Education Law Section 2-d]. See, Education Law Section 2-d(3)(c) and Part 121.3(c).

Nothing in Education Law Section 2-d or Part 121 requires an educational agency to post its third-party contracts on its website in their entirety. In addition, nothing in Education Law Section 2-d or Part 121 requires an educational agency to include the "supplemental information" about each contract, within the contract itself.

However, many school districts and other educational agencies have considered it a best practice to include most or all of the required elements of "supplemental information" within each applicable contract, and have complied with the obligation to include the "supplemental information" for each applicable contract with their Bill of Rights, by posting the text from this page of this Exhibit from each applicable contract (or a link to this text) on their website in proximity to their Bill of Rights.

THIRD-PARTY CONTRACTS

A third-party contractor is any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other agreement for purposes of providing services to such agency, including but not limited to data management, conducting studies, or evaluation of publicly funded programs. To learn more about this requirement, agencies can review Part 121.2, 121.3, 121.6, 121.9, and 121.10 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Pre-Negotiations:

- ✓ Update Parents' Bill of Rights
- ✓ Adopt District Policy

Contracts:

- ✓ Include All Required Elements

REQUIRED CONTRACT ELEMENTS

CONFIDENTIALITY MAINTAINED
Contracts must require the confidentiality of shared protected data be maintained in accordance with law and the educational agency's policy.

DATA SECURITY AND PRIVACY PLAN
Contracts must include the third-party contractor's data security and privacy plan that is accepted by the educational agency. Required elements are outlined in 121.6. Plans must:

- **IMPLEMENTATION OF ALL REQUIREMENTS**
  Outline how the contractor will implement all state, federal, and local contract requirements, consistent with the agency's policy;
- **SECURITY PROTECTIONS**
  Specify the administrative, operational and technical safeguards and practices it has in place;
- **SUPPLEMENTAL INFORMATION COMPLIANCE**
  Demonstrate that it complies with the supplemental information requirements;
- **CONTRACTOR AND SUBCONTRACTOR TRAINING**
  Specify how employees and its assignees receive or will receive training on the laws governing data prior to receiving access;
- **SUBCONTRACTORS MANAGEMENT**
  Specify if the contractor will utilize sub-contractors and how it will manage sub-contractor relationships and contracts;
- **CYBER INCIDENT PLAN**
  Specify how the contractor will manage incidents including specifying any plans to identify incidents, and to notify the agency;
- **DATA TRANSFER AND DISPOSAL**
  Describe whether, how and when data will be returned or destroyed when the contract is terminated;
- **SIGNED COPY OF THE BILL OF RIGHTS**
  Include a signed copy of the parents bill of rights for data privacy and security.

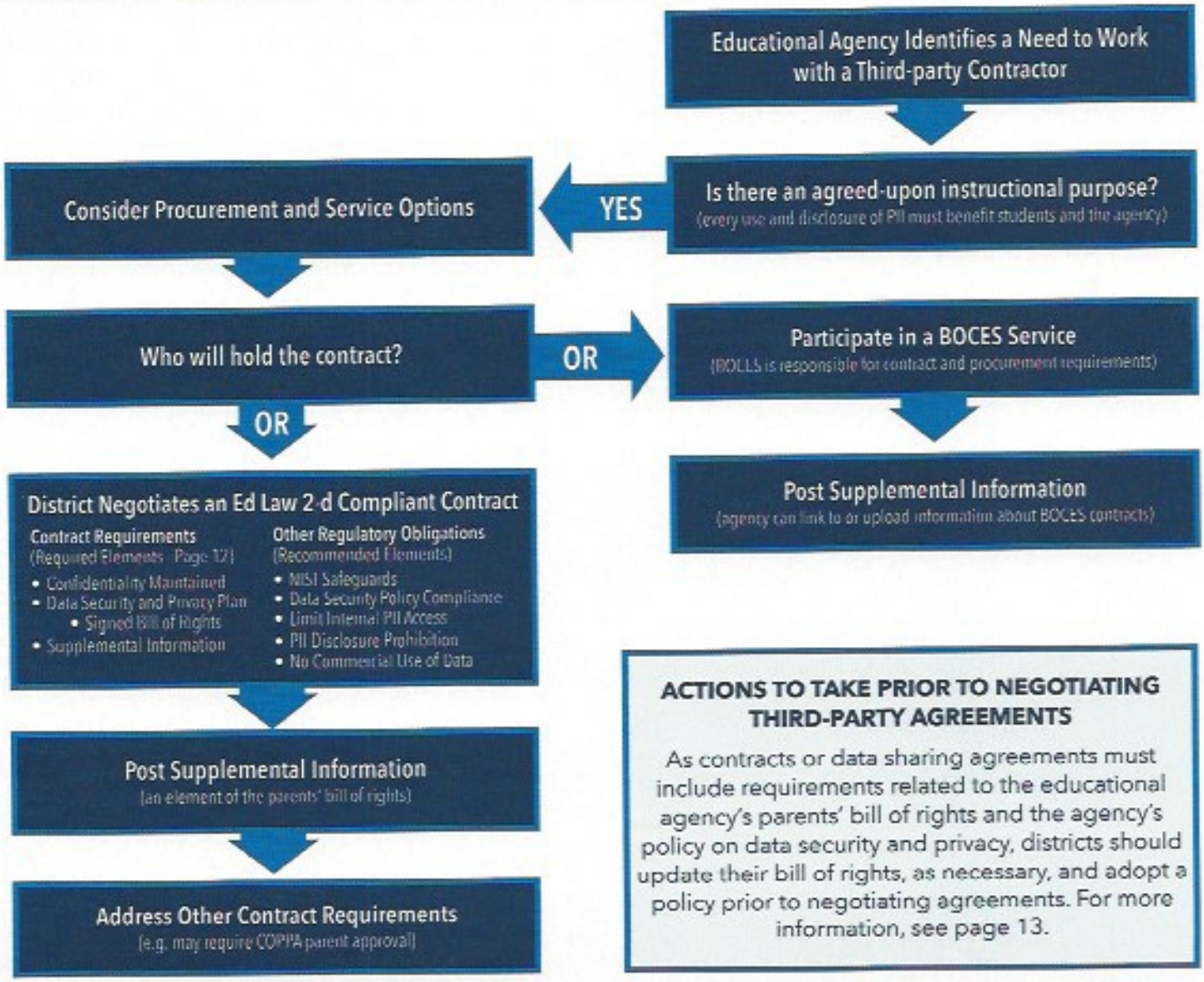
SUPPLEMENTAL INFORMATION
The bill of rights must include supplemental information for each third-party contract. See page 6, for more information.

THIRD-PARTY CONTRACTS AND PATHS TO COMPLIANCE

An agreement that covers the requirements defined by Ed Law 2-d must exist either directly between the school district and the product vendor, or, if the product is part of a service obtained through a BOCES CoSer, an agreement between that BOCES and the product vendor. A vendor cannot achieve compliance unilaterally.

If a district procures a product directly from a vendor, whether it is a paid platform or the district "signs up" for a free service, the district is entering into a contract with the vendor. Even though a compliant agreement may exist between a BOCES and a vendor, if a district does not obtain that vendor's product as part of a service delivered through a BOCES CoSer governed by that agreement, the BOCES-negotiated terms do not apply to that district.

TWO PATHS TO CONTRACTUAL COMPLIANCE



ACTIONS TO TAKE PRIOR TO NEGOTIATING THIRD-PARTY AGREEMENTS

As contracts or data sharing agreements must include requirements related to the educational agency's parents' bill of rights and the agency's policy on data security and privacy, districts should update their bill of rights, as necessary, and adopt a policy prior to negotiating agreements. For more information, see page 13.

STUDENT PII SAMPLE CONTRACT ADDENDUM

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. **Applicability of This Addendum**
The ____ School District ("DISTRICT") and ____ ("Vendor") are parties to a contract dated ____ ("the underlying contract") governing the terms under which DISTRICT accesses, and Vendor provides, [name of product(s) covered by contract] ("Product"). DISTRICT's use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. **Definitions**
   2.1 "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from DISTRICT or is created by the Vendor's product or service in the course of being used by DISTRICT.
   2.2 "Vendor" means [name of vendor identified above].
   2.3 "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes DISTRICT.
   2.4 DISTRICT" means the ____ School District.
   2.5 "Parent" means a parent, legal guardian, or person in parental relation to a Student.
   2.6 "Student" means any person attending or seeking to enroll in an educational agency.
   2.7 "Eligible Student" means a student eighteen years or older.
   2.8 "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.
   2.9 "This Contract" means the underlying contract as modified by this Addendum.

3. **Vendor Status**
Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. **Confidentiality of Protected Information**
Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the DISTRICT Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

STUDENT PII SAMPLE CONTRACT ADDENDUM

5. **Vendor Employee Training**
Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. **No Use of Protected Information for Commercial or Marketing Purposes**
Vendor warrants that Protected Information received by Vendor from DISTRICT or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. **Ownership and Location of Protected Information**

7.1 Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with DISTRICT. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2 DISTRICT shall have access to the DISTRICT's Protected Information at all times through the term of this Contract. DISTRICT shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3 Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by DISTRICT or its authorized users, or performing any other data analytics other than those required to provide the Product to DISTRICT. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back up must be provided to DISTRICT upon request.

7.4 All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. **Purpose for Sharing Protected Information**
The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT.

9. **Downstream Protections**
Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. **Protected Information and Contract Termination**

10.1 The expiration date of this Contract is defined by the underlying contract.

10.2 Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT.

10.3 Vendor shall thereafter securely delete and overwrite any and all Protected Information 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 of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4 Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5 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 removed) derived from Protected Information, they agree not to attempt to re-identify de identified data and not to transfer de-identified data to any party.

10.6 Upon request, Vendor and/or its subcontractors or assignees will provide a certification to DISTRICT from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. **Data Subject Request to Amend Protected Information**

11.1 In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2 Vendor will cooperate with DISTRICT in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. **Vendor Data Security and Privacy Plan**

12.1 Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2 Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

a. align with the NIST Cybersecurity Framework 1.0;

b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

c. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the DISTRICT data security and privacy policy (Attachment B);

d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

e. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

f. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

g. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

h. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify DISTRICT; and

i. describe whether, how and when data will be returned to DISTRICT, transitioned to a successor contractor, at DISTRICT's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. **Additional Vendor Responsibilities**

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the DISTRICT unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to DISTRICT no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data by the 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 but no more than seven calendar days after the discovery of the breach; and

13.7 Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse DISTRICT for the full cost incurred by DISTRICT to send notifications required by Education Law Section 2-d.

STUDENT PII SAMPLE CONTRACT ADDENDUM

Signatures

For ____ School District

For [Vendor Name]

_____ _____

President of the Board of Education

Date:

Date:

Attachment A - Parents' Bill of Rights for Data Security and Privacy

____ School District

Parents' Bill of Rights for Data Privacy and Security

[INSERT Parents' Bill of Rights for Data Privacy and Security]

For ____ School District

For [Vendor Name]

_____ _____

Superintendent

Date:

Date:

Supplemental Information About this Contract

[INSERT Supplemental Information. View an example on Page 9.]

Attachment B - District Policy

Attachment C - Vendor's Data Security and Privacy Plan

The DISTRICT Parents Bill of Rights for Data Privacy and Security, a signed copy of which is included as Attachment B to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

[INSERT Links or Text, as provided by the Vendor]

NIST CYBERSECURITY FRAMEWORK

Education Law 2-d requires educational agencies to adopt a policy on data security and privacy that aligns with the NIST Cybersecurity Framework, or NIST CSF. At the center of the NIST CSF is the Framework Core, which is a set of activities and desired outcomes to help organizations manage data security and privacy risk. Districts will use a Target Profile, Current Profile, and Action Plan to apply these activities. To learn more about this requirement, review Part 121.5 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

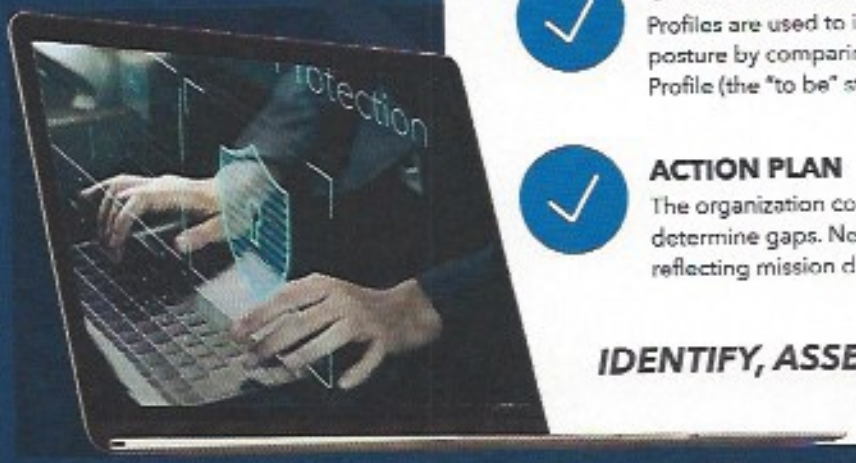
COMPLIANCE CHECKS

Policy:

- ✓ Aligns with the NIST CSF
- ✓ Is Adopted by October 1, 2020

Action Plan:

- ✓ Identifies Priority Action Items to Address Profile Gaps



NIST CSF VERSION 1.1 OVERVIEW

FRAMEWORK CORE
A set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors

FRAMEWORK CORE FUNCTIONS
The Core consists of five concurrent and continuous functions—Identify, Protect, Detect, Respond, Recover. These functions provide a high-level, strategic view of the organization's management of cybersecurity risk.

FRAMEWORK IMPLEMENTATION TIERS
Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

FRAMEWORK PROFILE
The Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories

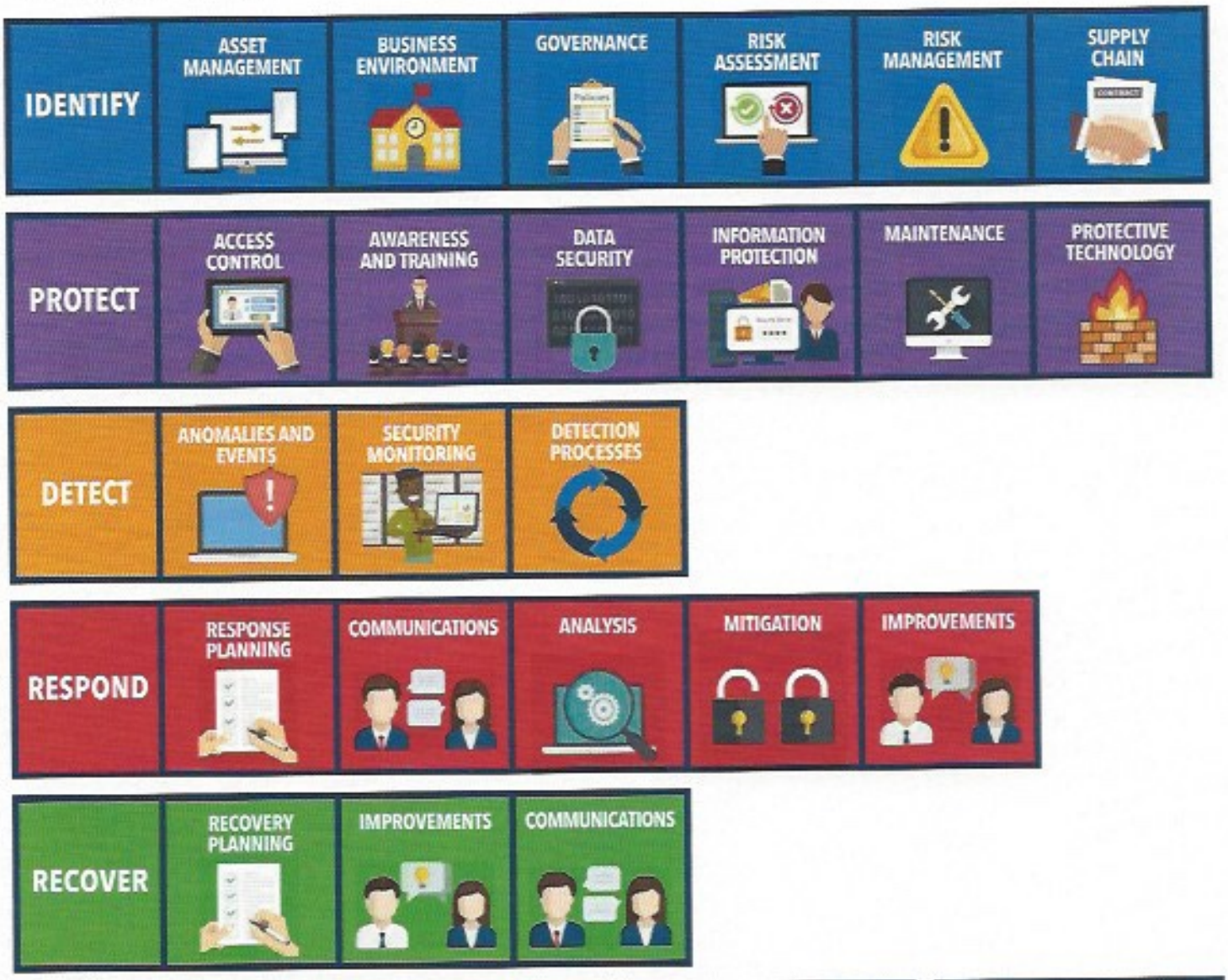
CURRENT PROFILE AND TARGET PROFILE
Profiles are used to identify opportunities for improving the cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).

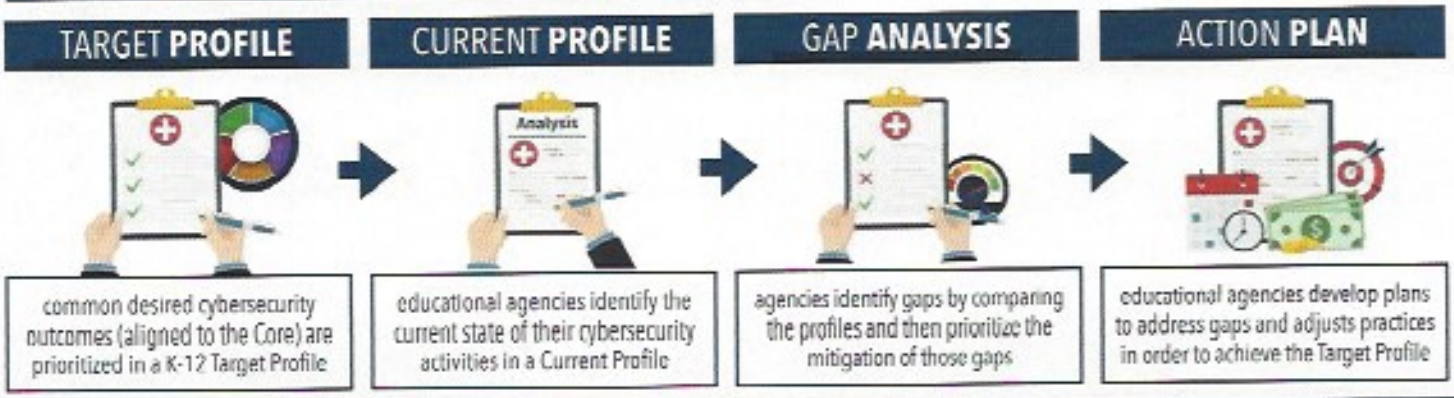
ACTION PLAN
The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks.

IDENTIFY, ASSESS, & MANAGE CYBER RISKS

NIST CSF CORE & PROFILE ACTION PLANNING DIAGRAMS

The Core is a set of desired cybersecurity activities organized into 5 functions, 23 categories, and 108 subcategories. Profiles, aligned to the Core, are used to identify opportunities for improving the cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).





ANNUAL EMPLOYEE TRAINING

Educational agencies are responsible for providing data privacy and security awareness training to their officers and employees with access to personally identifiable information annually. Training should include training on the state and federal laws, and how employees can comply with such laws. Each agency must also provide notice of the agency's data security and privacy policy to all its officers and employees. To learn more about this requirement, agencies can review 121.7 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Training:

- ✓ All Employees and Officers with Access to PII Trained Annually

Specialized Training:

- ✓ Review Section PR.AT of the NIST CSF (Targeted Staff Need Additional Training)

BEST PRACTICES

COMPLYING WITH STATE AND FEDERAL LAWS

Training on the state and federal laws that protect PII, and how employees can comply with such laws.

- **NEW YORK STATE EDUCATION LAW 2-D**
  This law protects the privacy and security of personally identifiable information (PII) of students, and certain APPR data. The law outlines requirements for educational agencies and their contractors.
  - **PROTECTED DATA**
    Employees need to know what types of information are protected.
  - **PARENTS' RIGHTS**
    Employees should be aware of the Bill of Rights. For example, parents have the right to inspect their child's education record.
  - **DISTRICT POLICY**
    Each agency must provide notice of the agency's data security and privacy policy to all its officers and employees.
  - **SECURITY AWARENESS TOPICS**
    The NIST CSF includes controls related to personnel being provided cybersecurity awareness education and trained to perform duties consistent with policies and agreements.
  - **REQUIREMENTS RELATED TO THIRD-PARTY CONTRACTOR**
    Employees must be informed that contracts created through clicking an "accept" agreement are subject to Ed Law 2-d if, as a result of using that contractor's product, the contractor receives protected PII from the agency.
  - **INCIDENT PROCEDURES**
    Employees must be informed of incident complaint, response, and notification requirements.
- **FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)**
  This is the foundational federal law related to the privacy of students' educational records. FERPA limits access to student records and details rules to follow when providing access to or disclosing the data.
- **CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)**
  COPPA imposes requirements on operators of websites, games, apps or online services directed to children under 13, and on online service providers that collect PII online from a child under 13.
- **PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA)**
  PPRA defines the rules states and districts must follow when administering surveys, analysis, and evaluations funded by the US Department of Education.

UNAUTHORIZED DISCLOSURE COMPLAINT

Educational agencies must establish and communicate to parents, eligible students, principals, teachers, and other staff of an educational agency procedures to file complaints about breaches or unauthorized releases of student data and/or protected teacher or principal data. To learn more about this requirement, agencies can review Part 121.4 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Complaint Procedures:

- ✓ Contain Required Elements
- ✓ Are Communicated to Parents and Staff

REQUIRED ELEMENTS

ACKNOWLEDGE, INVESTIGATE, AND CONTAIN
The agency must promptly acknowledge receipt, commence an investigation, and take the necessary precautions to protect PII.

PROVIDE FINDINGS
No more than 60 calendar days from the receipt of the complaint, the agency must provide the findings to the individual who filed a complaint.

MAINTAIN RECORDS
The agency must maintain a record of all complaints and their disposition in accordance with applicable data retention policies, including ED-1.

RELATED INFORMATION

PRIVACY COMPLAINTS CAN BE MADE TO NYSED
A complaint may be submitted to the Chief Privacy Officer using an online form at: http://www.nysed.gov/data-privacy-security/report-improper-disclosure

ED-1 (RECORDS RETENTION AND DESTRUCTION)
Information about ED-1 is available at: http://www.archives.nysed.gov/common/archives/files/mr_pub_ed1.pdf

EDUCATIONAL AGENCIES MAY REQUIRE COMPLAINTS TO BE SUBMITTED IN WRITING.

MODEL UNAUTHORIZED DISCLOSURE FORM

Parents, eligible students (students who are at least 18 years of age), principals, teachers, and employees of an educational agency may file a complaint about a possible breach or improper disclosure of student data and/or protected teacher or principal data using this form. Submit this form to [insert submission information]. Please do NOT include any information in this form that would constitute student personally identifiable information.

CONTACT INFORMATION

First Name:

Last Name:

Phone Number:

Email:

Role/Relationship to Student:

District/Building Affiliation:

POSSIBLE IMPROPER DISCLOSURE OR BREACH INFORMATION

Description of Event(s):

Description of Possible Disclosed Data:

Description of How Reporter Learned of Possible Disclosure:

FOR DISTRICT USE ONLY

Date Received:

Staff Member Responsible for Investigation:

Findings Communication Date:

Signature to Confirm Investigation Complete:

MODEL IMPROPER DISCLOSURE NOTIFICATION

This letter is to inform you of an incident that occurred within the [insert system]. This incident resulted in student/staff/etc data being accessed without authorization by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation.

[insert required elements:

- a brief description of the breach or unauthorized release
- the dates of the incident and the date of discovery
- a description of the types of personally identifiable information affected
- an estimate of the number of records affected
- a brief description of the educational agency's investigation or plan to investigate]

Please know that our district is committed to protecting and securing educational data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your child's educational records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident occurring in the future. Please contact [insert name] with any questions you may have regarding this incident and our response [Note: The regulations require agencies to include contact information for representatives who can assist parents].

MODEL UNAUTHORIZED RELEASE COMPLAINTS RECORD

The agency must maintain a record of all complaints and their disposition in accordance with applicable data retention policies, including ED-1. Insert information about complaints into the log.

COMPLAINANT NAME	DATE COMPLAINT SUBMITTED
DESCRIPTION OF THE COMPLAINT	
FINDINGS	
DATE THE FINDING REPORT WAS SHARED WITH COMPLAINANT	

INCIDENT REPORTING AND NOTIFICATION

Educational agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer and notify impacted stakeholders. To learn more about this requirement, agencies can review Part 121.10 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Incident Response Procedures:

- ✓ Outlines All Required Actions

Contracts:

- ✓ Outline All Third-Party Contractor Requirements

REPORTING REQUIREMENTS

10 DAYS TO REPORT TO NYSED
The agency must report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer no more than 10 calendar days after such discovery.

NOTIFICATION REQUIREMENTS

60 DAYS TO NOTIFY AFFECTED INDIVIDUALS
The agency must notify affected parents, eligible students, teachers and/or principals no more than 60 calendar days after the discovery of a breach or unauthorized release.

LAW ENFORCEMENT OR VULNERABILITY DELAY
Where notification is delayed, the agency must notify affected individuals within 7 calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

THIRD-PARTY REIMBURSEMENT REQUIREMENT
Where a breach or unauthorized release is attributed to a third-party contractor, the contractor must pay for or reimburse the agency for the full cost of notification.

METHOD OF NOTIFICATION
Notification must be directly provided to the affected individuals by first-class mail to their last known address; by email; or by telephone.

CONTENTS OF NOTIFICATION
Notifications must be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

- a brief description of the unauthorized release
- the dates of the incident and date of discovery
- a description of the types of PII affected
- the number of records affected
- a brief description of the agency's investigation
- contact information for representatives who can assist parents