

PROPOSED PART 121

OF THE COMMISSIONER'S REGULATIONS

IMPLEMENTING EDUCATION LAW 2-D



PROTECTING PERSONALLY IDENTIFIABLE INFORMATION



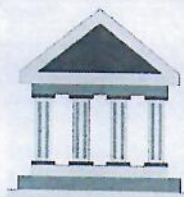
BOARD OF REGENTS
PRESENTATION

JAN 14, 2019



PUBLIC SUBMITS
FEEDBACK

JAN 30 - MARCH 30



BOARD OF REGENTS
CONSIDERS ADOPTION

JUNE 2019



REGULATIONS
EFFECTIVE

JULY 1, 2019



EDUCATIONAL AGENCIES
ADOPT DATA SECURITY AND
PRIVACY POLICY

DEC 31, 2019

DEVELOPED BY:



CREATED:

Version 2

May 2019

NYS RICS OVERVIEW:

12 NYS centers organized under and supporting the 37 BOCES to provide shared technology services.

PROPOSED PART 121 REQUIREMENTS OVERVIEW

Following this page, there is a one-page resource related to each of the requirements noted below.

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)



Regulations
121.2 and
121.5

Protect the confidentiality of personally identifiable information of students (FERPA) and personally identifiable information of teachers and principals (APPR)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY



Regulations
121.3

Adopt and post on website a Parents Bill of Rights for Data Privacy and Security, with supplemental information about each written agreement with a third-party contractor (vendor) that involves disclosure of PII

DATA SECURITY AND PRIVACY POLICY



Regulations
121.5

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

NIST CYBERSECURITY FRAMEWORK



Regulations
121.5

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

THIRD-PARTY CONTRACTS



Regulations
121.2, 121.3,
121.6, 121.9,
121.10

Whenever the educational agency discloses PII to a third-party contractor, ensure that the written agreement for using the product or services includes the language required by Education Law

ANNUAL EMPLOYEE TRAINING



Regulations
121.5 and
121.7

Deliver annual privacy and security awareness training to all employees

PARENT COMPLAINT PROCEDURES



Regulations
121.4

Create and publish a parent complaint process

INCIDENT REPORTING AND NOTIFICATION



Regulations
121.10

Follow reporting and notification procedures when unauthorized disclosure occurs

DATA PROTECTION OFFICER



Regulations
121.8

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

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)



Districts leverage data to advance the goals of improving academic achievement, empowering parents and students with information, and advancing efficient and effective school operations. **Districts need to balance these benefits and the responsibility to minimize the collection and transmission of PII in order to reduce risk.** Specifically, educational agencies must ensure that every use of PII by the educational agency benefits students. Additionally, educational agencies can not sell or disclose PII for commercial purposes. To learn more about this requirement, agencies can review Part 121.2 and 121.5 of the Regulations.

PERSONALLY IDENTIFIABLE INFORMATION

Personally identifiable information (PII) includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

 STUDENT NAME	 PARENT'S NAME	 STUDENT ADDRESS	 STUDENT NUMBER	 LINKABLE INFORMATION
--	---	---	--	--

DISCLOSURE AVOIDANCE PROCEDURES

Educational Agencies must ensure personally identifiable information is not included in public reports or other documents.

Disclosure avoidance procedures are efforts made to protect PII in aggregate reports and public documents. These strategies reduce the risk of disclosure of PII. The diagram to the right highlights three commonly used disclosure avoidance methods. To learn more about disclosure avoidance practices, agencies can

visit <https://studentprivacy.ed.gov/>. This website is a service of the U.S. Department of Education's Privacy Technical Assistance Center and the Family Policy Compliance Office.



DISCLOSURE AVOIDANCE PRACTICES

SUPPRESSION



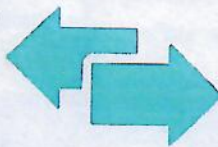
Involves removing data to prevent identification of small groups

BLURRING



Involves reducing the precision of the disclosed data to minimize identification

PERTURBATION



Involves making small changes to the data to prevent identification of unique groups

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY



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 table below highlights required terms 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.

 <p>DATA WILL NOT BE SOLD AND WILL NOT BE RELEASED FOR COMMERCIAL PURPOSES</p>	 <p>INSPECTING RECORD RIGHT TO REVIEW CHILD'S EDUCATION RECORD</p>	 <p>DATA IS PROTECTED BY LAW AND SAFEGUARDS MUST BE IN PLACE</p>	 <p>NYSED COLLECTED DATA LINK TO DEPARTMENT LISTING OF COLLECTED DATA ELEMENTS</p>	 <p>BREACH COMPLAINT CONTACT PERSON FOR PARENTS</p>
--	--	--	---	---

INFORMATION ABOUT THIRD-PARTY CONTRACTS

Educational agencies are required to **post information about third-party contracts on the agency's website** with the Parents Bill of Rights. The table below highlights the supplemental information that agencies are required to post. 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.

CONTRACTOR AND PRODUCT NAME	
EXCLUSIVE PURPOSES FOR DATA USE	DATA ACCURACY/CORRECTION PRACTICES
The exclusive purposes for which the student data [or teacher or principal data] will be used by the third-party contractor include _____.	Parent, [student, eligible student, teacher or principal] may challenge the accuracy of the data by _____.
SUBCONTRACTOR OVERSIGHT DETAILS	SECURITY PRACTICES
<p>This contract has no subcontractors. OR</p> <p>The contractor will ensure subcontractors abide by data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations by _____.</p>	<ul style="list-style-type: none"> The data is stored _____. The security protections taken to ensure data will be protected include _____.
CONTRACT LIFECYCLE PRACTICES	ENCRYPTION PRACTICES
<ul style="list-style-type: none"> The agreement expires _____. When the agreement expires, the student data [or teacher or principal data] will be _____. 	Data encryption is applied in accordance with Education Law §2-d 5(f)(5).

DATA SECURITY AND PRIVACY POLICY



Education Law 2-d requires educational agencies to adopt a policy on data security and privacy by December 31, 2019. The chart below highlights some of the components that will be addressed in this policy and related procedures. Additionally, the law requires educational agencies to publish the policy on the district's website. To learn more about this requirement, agencies can review Part 121.5 of the Regulations.

DATA SECURITY AND PRIVACY POLICY SAMPLE AREAS OF FOCUS

 <p>NIST CSF ALIGNED PRACTICES NIST Cybersecurity Framework aligned practices</p>	 <p>DATA GOVERNANCE ensure every use of PII benefits students and the agency</p>	 <p>DISCLOSURE AVOIDANCE protection of PII in public reports</p>	 <p>STATE AND FEDERAL LAWS FERPA, IDEA, and other laws</p>
 <p>DATA PROTECTION OFFICER employee responsible for the implementation of the policies</p>	 <p>ANNUAL EMPLOYEE TRAINING privacy and security awareness training</p>	 <p>PARENT COMPLAINT PROCEDURES complaints about breaches or unauthorized releases of student data</p>	 <p>INCIDENT REPORTING AND NOTIFICATION report the breach to the NYSED CPO and impacted stakeholders</p>

POLICY IMPLEMENTATION TIMELINE



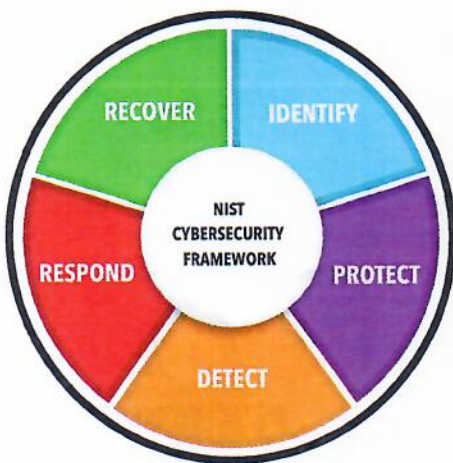
NIST CYBERSECURITY FRAMEWORK



Education Law 2-d requires educational agencies to adopt a policy on data security and privacy that aligns with the state's 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 designed to help organizations manage data security and privacy risk.** Districts will use the Target Profile, Current Profile, and Action Plan, described below, to apply these activities. To learn more about this requirement, agencies will review the NYS K-12 Target Profile, supplemental resources and Part 121.5 of the Regulations.

MAIN COMPONENTS OF THE CYBERSECURITY FRAMEWORK

NIST FRAMEWORK CORE



The Core is a set of **SPECIFIC ACTIVITIES TO MANAGE DATA SECURITY AND PRIVACY RISK**. The Core is organized into functions, categories, and subcategories.



PROFILES AND EDUCATIONAL AGENCY ACTION PLANS

TARGET PROFILE



STATE NYS K-12 TARGET PROFILE DEVELOPED

common desired cybersecurity outcomes are prioritized in the NYS K-12 Target Profile

CURRENT PROFILE



AGENCIES DETERMINE THEIR CURRENT PROFILE

educational agencies identify the current state of their cybersecurity activities in the Current Profile

GAP ANALYSIS



AGENCIES ANALYZE AND PRIORITIZE GAPS

agencies identify gaps by comparing the profiles and then prioritize the mitigation of those gaps

ACTION PLAN



AGENCIES DEVELOP AND IMPLEMENT ACTION PLANS

educational agencies develop plans to address gaps and adjust practices in order to achieve the Target Profile

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 written agreement** for purposes of providing services to such educational 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.



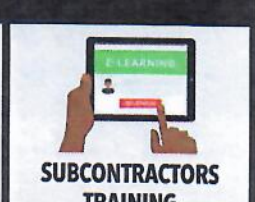
Agreements created in electronic form and signed with an electronic or digital signature or **CLICKWRAP AGREEMENTS** used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service **ARE SUBJECT TO EDUCATION LAW 2-D REQUIREMENTS.**

OVERVIEW OF REQUIREMENTS RELATED TO THIRD-PARTY CONTRACTORS

CONFIDENTIALITY MAINTAINED



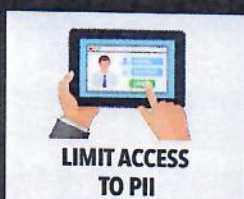
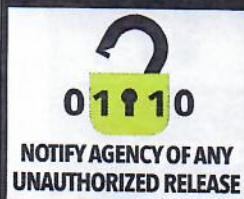
DATA SECURITY AND PRIVACY PLAN



OBLIGATIONS RELATED TO THE SUPPLEMENTAL INFORMATION FOR PARENTS BILL OF RIGHTS



ADDITIONAL STATUTORY AND REGULATORY OBLIGATIONS



ANNUAL EMPLOYEE TRAINING



Educational agencies shall **annually provide information privacy and security awareness training to their employees with access to personally identifiable information**. To learn more about this requirement, agencies can review Part 121.5 and 121.7 of the Regulations.

SUGGESTED PRIVACY AND SECURITY AWARENESS TRAINING TOPICS

	<h3>LAWS, POLICIES, AND PROCEDURES</h3>
	<ul style="list-style-type: none"> • Data Security and Privacy Policy • Incident Reporting • Laws and Regulations • Click Wrap Agreements <h3>SECURITY AWARENESS</h3> <ul style="list-style-type: none"> • Common Threats • Phishing Recognition • Social Engineering

K-12 THREAT LANDSCAPE

As educational agencies assess employee training needs, the most prominent NYS K-12 threat categories should be considered. This information can also inform agencies' NIST align Cybersecurity Action Plans.

SYSTEM AVAILABILITY	DATA INTEGRITY	UNAUTHORIZED PII DISCLOSURE	FINANCIAL THEFT
<p>Access to systems or infrastructure is disrupted or denied</p>	<p>Unauthorized data modification causing inaccuracy of information</p>	<p>PII viewed by unauthorized persons via theft or accidental leakage</p>	<p>Monetary loss due to digital theft, social engineering, or extortion</p>

These four areas were identified based on information from the following resources: Verizon Data Breach Investigations Report, Gartner Research, Homeland Security/US-Cert/CIS/MS-ISAC, NYS Troopers, FBI, NYS Office of Information Technology Services, NYS Comptroller Audit Findings, K-12 Cybersecurity Resource Center, PTAC, CoSN, Ponemon Institute Cost of Data Breach Report, Microsoft Security Intelligence Report, Data Quality Campaign, Statewide RIC Data, and Global News Outlets.

PARENT COMPLAINT PROCEDURES



Educational agencies must **establish and communicate to parents** and eligible students **procedures to file complaints about breaches or unauthorized releases of student data**. To learn more about this requirement, agencies can review Part 121.4 of the Regulations.

PARENT COMPLAINTS SUBMISSION PROCEDURE



Procedures to support parents submission of complaints of breach and unauthorized release of PII

DISTRICT INVESTIGATION AND NOTIFICATION PROCEDURE



Procedures to support the investigation of complaints and the communication of findings within 30 calendar days

DISTRICT MAINTENANCE OF RELATED RECORDS



Procedures to support record retention of all complaints and their disposition

MODEL COMPLAINT LOG

COMPLAINANT NAME

DATE COMPLAINT SUBMITTED

DESCRIPTION OF THE COMPLAINT

FINDINGS

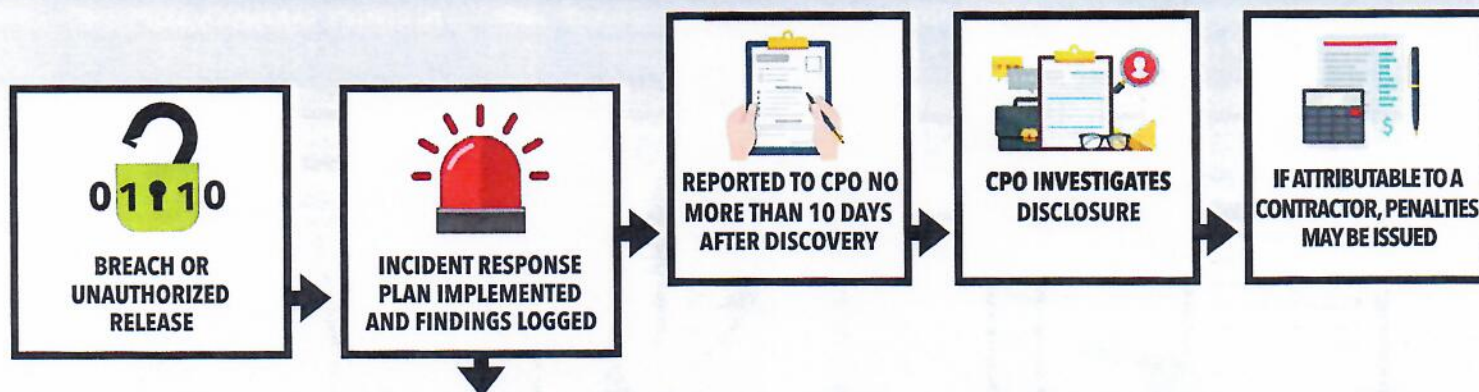
DATE THE FINDING REPORT WAS SHARED WITH COMPLAINANT

INCIDENT REPORTING AND NOTIFICATION

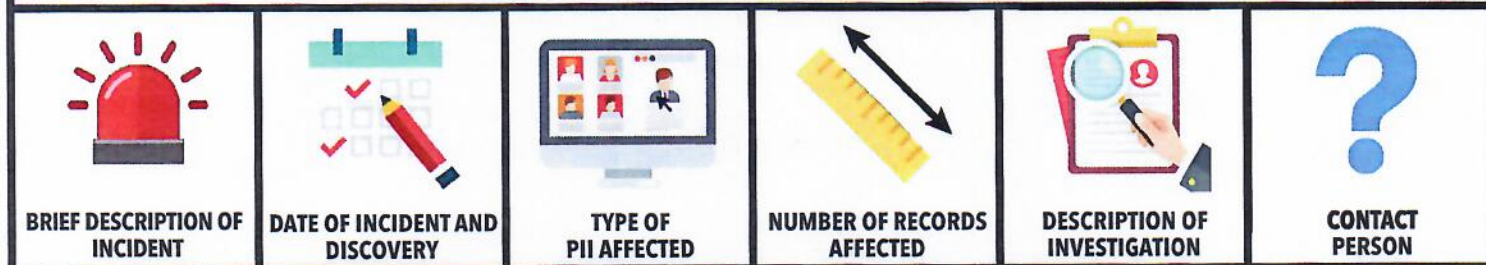


Upon the discovery of a breach, whether or not related to a third-party contractor or attributable to the actions of the educational agency, **the agency that is party to the contract must report the breach to the NYSED Chief Privacy Officer and impacted stakeholders.** To learn more about this requirement, agencies can review Part 121.10 of the Regulations.

EDUCATIONAL AGENCY INCIDENT REPORTING AND NOTIFICATION STEPS



AGENCY NOTIFIES IMPACTED FAMILIES AND STAFF NO MORE THAN 14 DAYS AFTER DISCOVERY



MODEL PARENT / STAFF INCIDENT NOTIFICATION LETTER

This letter is to inform you of an incident that occurred within the [insert system]. This incident resulted in student/staff/etc data being compromised by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation.

[insert 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.

DATA PROTECTION OFFICER



Each educational agency must **designate one or more data protection officer(s)**. **These leaders will be responsible for** the implementation of the policies and **procedures required in Education Law Section 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.

POTENTIAL RESPONSIBILITIES, QUALIFICATIONS, AND CONSIDERATIONS

Job Responsibilities:

- Serve as the point of contact for data security and privacy for the educational agency, and as a liaison for the State Education Department's Chief Privacy Officer.
- Implement the policies and procedures required in Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education, reporting issues to the Superintendent.
- Monitor the educational agency's compliance with state and federal information security and privacy laws and regulations.
- Evaluate technologies, projects, and initiatives, and support the negotiation of privacy and security terms and conditions into contracts with third-party contractors.
- Develop and maintain the educational agencies Data Security and Privacy Action Plan.
- Manage data security and privacy training, education, and awareness for staff.
- Advise and counsel administration and the Board of Education on best practices, new technologies, privacy complaints, and potential agency risks.
- Develop and maintain an incident response plan.
- Assist with investigations and responses to breaches or unauthorized releases of student data.

Preferred Knowledge, Skills and Abilities:

- Ability to gain a working knowledge of related laws and information security and privacy concepts.
- Strong communication skills (both written and oral).
- Excellent understanding of project management principles.
- Strong interpersonal skills.

Organizational Relationships:

- Reports to the Superintendent.
- As the Data Protection Officer may have other technology, data, or leadership duties, structures are implemented to address conflicts of interest.

