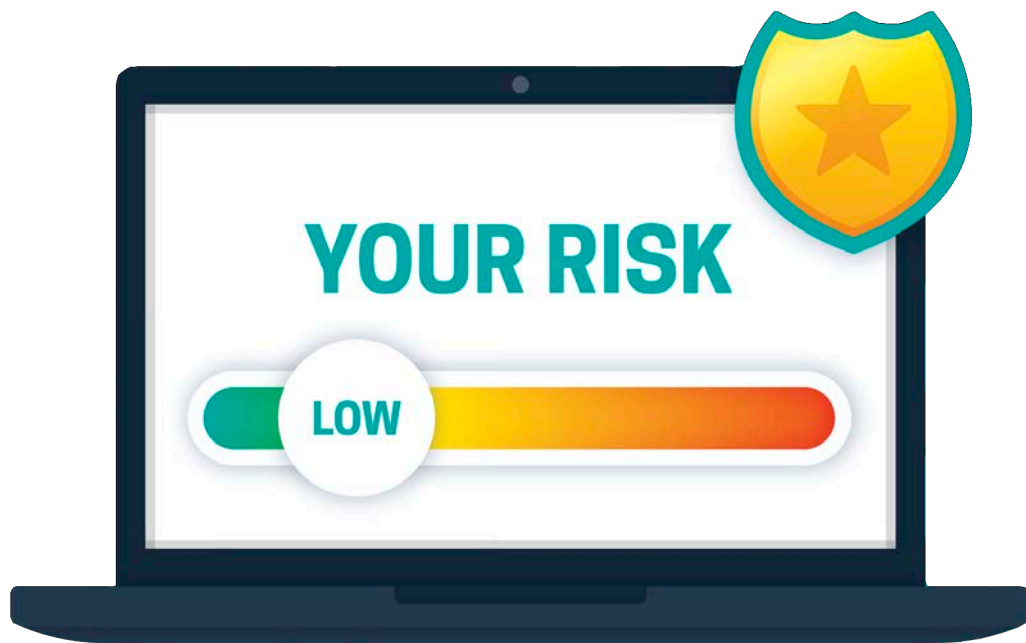


PROPOSED PART 121

OF THE COMMISSIONER'S REGULATIONS

IMPLEMENTING EDUCATION LAW 2-D



STRENGTHENING DATA PRIVACY AND SECURITY IN NY STATE EDUCATIONAL AGENCIES TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION



INITIAL DRAFT REGULATIONS
PRESENTED TO BOARD OF
REGENTS

JAN 2019



PUBLIC SUBMITS FEEDBACK
AND REGULATIONS REFINED

JAN 2019 - DEC 2019



BOARD OF REGENTS CONSIDERS
ADOPTION

JAN 2020



EDUCATIONAL AGENCIES ADOPT
DATA SECURITY AND PRIVACY
POLICY

JULY 1, 2020

DEVELOPED BY:



VERSION DATE:

OCTOBER 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)
----------------------------------------------------------------------------------	-----------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------

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
------------------------------------------------------------------------------------	-----------------------------------	-------------------------------------------------------------------------

UNAUTHORIZED DISCLOSURE COMPLAINT PROCEDURES

	Regulations 121.4	Create and publish a unauthorized disclosure 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.



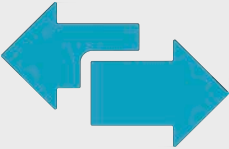
 <p>STUDENT NAME</p>	 <p>PARENTS' NAMES</p>	 <p>STUDENT ADDRESS</p>	 <p>STUDENT NUMBER</p>	 <p>LINKABLE INFORMATION</p>
--------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------

DISCLOSURE AVOIDANCE PROCEDURES

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

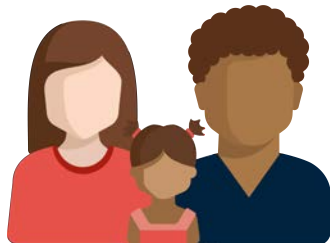
Disclosure avoidance procedures are efforts made to protect PII in aggregate reports and public documents. These strategies reduce the risk of disclosure of PII. The diagram to the right highlights three commonly used disclosure avoidance methods. To learn more about disclosure avoidance practices, agencies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



DISCLOSURE AVOIDANCE PRACTICES	<p>SUPPRESSION</p> 	<p>Involves removing data to prevent identification of small groups</p>
	<p>BLURRING</p> 	<p>Involves reducing the precision of the disclosed data to minimize identification</p>
	<p>PERTURBATION</p> 	<p>Involves making small changes to the data to prevent identification of unique groups</p>

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

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY



A **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 Bill of Rights. The table below provides an example of supplemental information. 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
<p>The exclusive purposes for which the student data [or teacher or principal data] will be used by the third-party contractor include _____.</p>	<p>Parents and eligible students can challenge the accuracy of any student data by following the school district's procedure for requesting the amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers and principals may challenge the accuracy of APPR data by following the appeal procedure in the school district's APPR Plan.</p>
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 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 _____. 	<p>Data encryption is applied in accordance with Education Law §2-d.</p>

DATA SECURITY AND PRIVACY POLICY








Education Law 2-d requires educational agencies to adopt a policy on data security and privacy by July 1, 2020. 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 educational 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>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

 <p>NYSED MODEL POLICY AVAILABLE</p>	 <p>LOCAL MODEL POLICIES AVAILABLE</p>	 <p>EDUCATIONAL AGENCY ADOPTS DATA SECURITY AND PRIVACY POLICY</p>	 <p>POLICY IS POSTED ON WEBSITE AND NOTICE PROVIDED TO OFFICERS AND EMPLOYEES</p>	 <p>DATA PROTECTION OFFICER MONITORS COMPLIANCE</p>
<p>WINTER 2019</p>	<p>WINTER 2019</p>	<p>BY JULY 1, 2020</p>	<p>BY JULY 1, 2020</p>	<p>ONGOING</p>

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 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

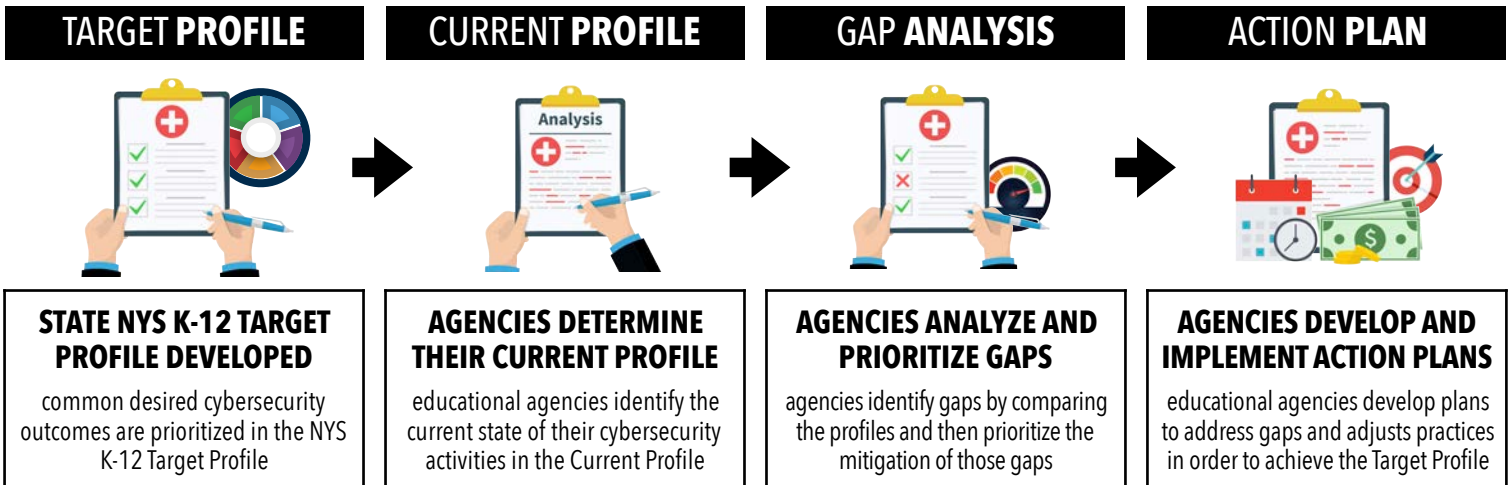
NIST FRAMEWORK CORE



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

IDENTIFY	ASSET MANAGEMENT	ENVIRONMENT	GOVERNANCE	RISK ASSESSMENT	RISK MANAGEMENT	CONTRACTORS MANAGEMENT
PROTECT	IDENTITY MANAGEMENT	AWARENESS AND TRAINING	DATA SECURITY	INFORMATION PROTECTION	MAINTENANCE	PROTECTIVE TECHNOLOGY
DETECT	ANOMALIES AND EVENTS	SECURITY MONITORING	DETECTION PROCESSES			
RESPOND	RESPONSE PLANNING	COMMUNICATION	ANALYSIS	MITIGATION	IMPROVEMENTS	
RECOVER	RECOVERY PLANNING	IMPROVEMENTS	COMMUNICATION			

PROFILES AND EDUCATIONAL AGENCY ACTION PLANS



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

DATA SECURITY AND PRIVACY PLAN

 IMPLEMENTATION OF ALL REQUIREMENTS	 SECURITY PROTECTIONS	 SUPPLEMENTAL INFO COMPLIANCE
 CONTRACTOR TRAINING	 SUBCONTRACTOR TRAINING	 SUBCONTRACTORS MANAGEMENT
 CYBER INCIDENT PLAN	 DATA TRANSFER AND DISPOSAL	 SIGNED COPY OF THE BILL OF RIGHTS

ADDITIONAL STATUTORY AND REGULATORY OBLIGATIONS

 NIST CSF SAFEGUARDS	 COMPLY WITH AGENCY POLICY AND LAW 2-D	 LIMIT ACCESS TO PII
 ONLY USE PII AS AUTHORIZED	 NOT DISCLOSE PII TO ANY OTHER PARTY	 SAFEGUARD THE PII IN CUSTODY
 ENCRYPTION PRACTICES APPLIED	 PROHIBITIONS ON PII COMMERCIAL USE	 OVERSIGHT OF SUBCONTRACTOR

OBLIGATIONS RELATED TO THE SUPPLEMENTAL INFORMATION FOR THE BILL OF RIGHTS

 EXCLUSIVE PURPOSES FOR DATA USE	 OVERSIGHT OF SUBCONTRACTORS	 CONTRACT DURATION AND DATA DISPOSAL	 DATA ACCURACY / CORRECTION PRACTICES	 SECURITY PROTECTIONS AND DATA LOCATION	 ENCRYPTION PRACTICES APPLIED
--------------------------------------------	----------------------------------------	------------------------------------------------	-------------------------------------------------	---------------------------------------------------	-----------------------------------------

CONFIDENTIALITY MAINTAINED

 IN ACCORDANCE WITH LAWS	 IN ACCORDANCE WITH AGENCY POLICY
------------------------------------	---------------------------------------------

- Contractual Obligations
- Additional Statutory and Regulatory Obligations

ANNUAL EMPLOYEE TRAINING



Educational agencies shall **annually provide data privacy and security awareness training** to their officers and **employees with access to personally identifiable information**. Training should include training on the state and federal laws, and how employees can comply with such laws. 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.

<h3>SYSTEM AVAILABILITY</h3> <p>Access to systems or infrastructure is disrupted or denied</p>	<h3>DATA INTEGRITY</h3> <p>Unauthorized data modification causing inaccuracy of information</p>	<h3>UNAUTHORIZED PII DISCLOSURE</h3> <p>PII viewed by unauthorized persons via theft or accidental leakage</p>	<h3>FINANCIAL THEFT</h3> <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.

UNAUTHORIZED DISCLOSURE COMPLAINT PROCEDURES



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.

COMPLAINTS SUBMISSION PROCEDURE



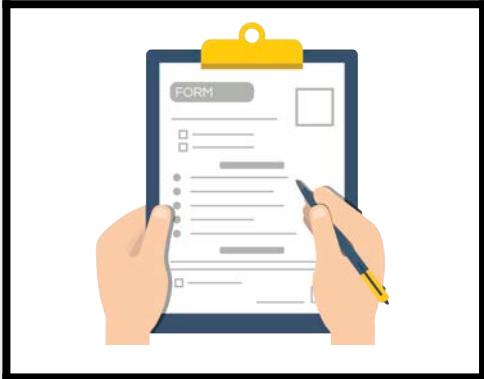
Procedures to support submission of complaints of breach and unauthorized release of PII

DISTRICT INVESTIGATION AND NOTIFICATION PROCEDURE



Procedures to support the investigation of complaints and the communication of findings within 60 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



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.

EDUCATIONAL AGENCY INCIDENT REPORTING AND NOTIFICATION STEPS



AGENCY NOTIFIES IMPACTED FAMILIES AND STAFF NO MORE THAN 60 DAYS AFTER DISCOVERY					
BRIEF DESCRIPTION OF INCIDENT	DATE OF INCIDENT AND DISCOVERY	TYPE OF PII AFFECTED	NUMBER OF RECORDS AFFECTED	DESCRIPTION OF INVESTIGATION	CONTACT PERSON

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 a Data Protection Officer** 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.

POTENTIAL RESPONSIBILITIES, QUALIFICATIONS, AND CONSIDERATIONS

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

