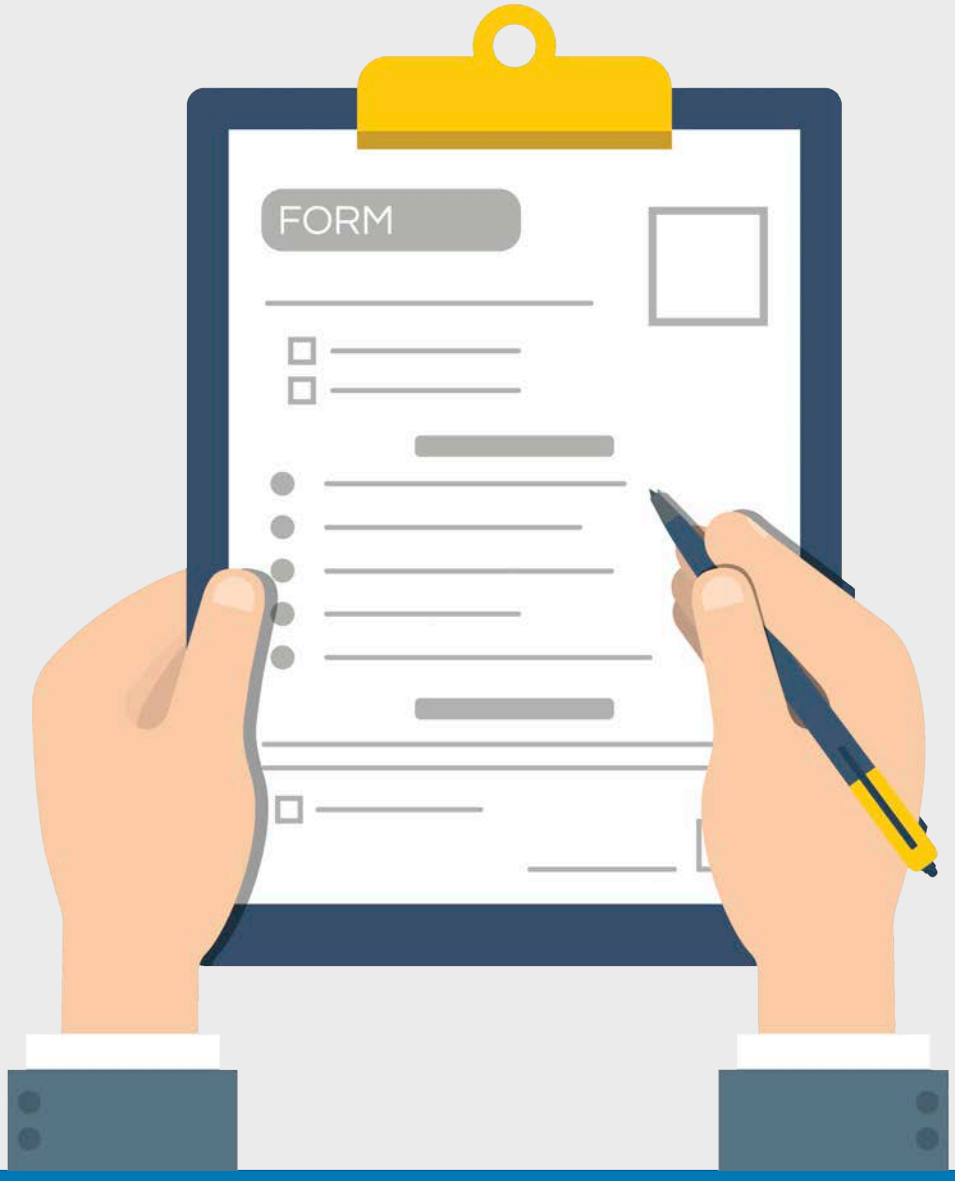
PART 121

OF THE COMMISSIONER'S REGULATIONS

IMPLEMENTATION TOOLKIT



IMPLEMENTATION TOOLS FOR EDUCATIONAL AGENCIES

DEVELOPED BY:

RIC one
TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE

VERSION DATE:

June 2020

ELECTRONIC VERSION:

HTTPS://RICONEDPSS.ORG/RESOURCES

NYS RICS OVERVIEW:

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

PROJECT MANAGEMENT TOOL

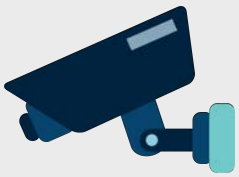
RESOURCE DEVELOPED BY: RIC one — TWELVE REGIONAL INFORMATION CENTERS WORKING AS ONE

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 PART	TIMELINE	COMPLETE
PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION	Guidelines for Personally Identifiable Information Utilization Defined and Communicated to all Staff	121.2 121.5 121.7		☐
BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY	Parents' Bill of Rights Published on District Website	121.3		☐
	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	By Oct 1, 2020	☐
NIST CYBERSECURITY FRAMEWORK	NIST CSF Aligned 2019-2020 Current Profile Developed	121.5		☐
	NIST CSF Aligned Security and Privacy Plan (Profile and 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		☐
	Terms and Conditions Negotiated into Contracts with Third-Party Contractors			☐
ANNUAL EMPLOYEE TRAINING	Employee Training Implemented	121.7		☐
UNAUTHORIZED DISCLOSURE COMPLAINT PROCEDURES	Complaint Procedures Defined	121.4		☐
	Breach, Unauthorized Release, and Complaint Record Maintained			☐
INCIDENT REPORTING AND NOTIFICATION	Incident Reporting and Notification Procedures and Forms Developed	121.10		☐
DATA PROTECTION OFFICER	Data Protection Officer Designated or Appointed	121.8		☐

PROTECTION OF PII ANALYSIS

Review and refine the example list of district systems that house the most sensitive information. For each system, specify the strategies in place to support the protection of that information.

SYSTEM CATEGORY	SYSTEM TYPE	SECURITY PRACTICES				
		ACCESS CONTROLS	MAINTENANCE MANAGEMENT	LOG REVIEW	SECURITY MONITORING	BACKUP PRACTICES
STUDENT 	**Student**					
	Cafeteria					
	NYSED Data Warehouse					
STAFF 	**Financial**					
	Educator Management					
MANAGEMENT 	**Security and Facilities**					
	Board Document Management					

This resource is relevant to the PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) Part 121 of the Commissioner's Regulations Requirements.

COMMON SUPPLEMENTAL INFORMATION LANGUAGE

Educational agencies are required to post information about third-party contracts on the agency's website with the Bill of Rights. Using the starter language below, identify current gaps and discuss how you are going to develop standard / common supplemental information contractual language for your school district.

CONTRACTOR AND PRODUCT NAME
EXCLUSIVE PURPOSES FOR DATA USE
The **exclusive purposes** for which the student data [or teacher or principal **data**] **will be used by the third-party contractor include** [insert the purposes defined in contract].
SUBCONTRACTOR OVERSIGHT DETAILS
[insert contractor name] will **ensure that any subcontractors**, assignees, or other agents who see or receive this protected data are **contractually required to obey the same data protection and security requirements** that [insert contractor name] is **required to obey under state and federal law**.
CONTRACT LIFECYCLE PRACTICES
The **contract expires on** [insert date] unless earlier renewed or automatically extended for a 12- month period pursuant to the agreement. **When the contract expires, protected data will, upon the written request** of the school district, **be deleted** by [insert contractor name], **and may be exported for use by** the [insert district name] **before being deleted**.
DATA ACCURACY/CORRECTION PRACTICES
Parents can challenge the accuracy of any student data stored by [insert district name] in a [insert contractor name] Product or Service **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 be able to challenge the accuracy of APPR data stored by [insert district name] in a [insert third contractor name] Product or Service by following the appeal procedure in the school district's APPR Plan.
SECURITY PRACTICES
Protected data provided to [insert contractor name] by a participating school district **will be stored** [insert location]. The **measures** that [insert third party contractor name] takes **to protect** student data and teacher and principal **data** will **align with the NIST Cybersecurity Framework and industry best practices** including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
ENCRYPTION PRACTICES
Data encryption will be employed at least to the extent required by Education Law Section 2-d.

This resource is relevant to the BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY Part 121 of the Commissioner's Regulations Requirements.

DATA SECURITY AND PRIVACY POLICY

As required by Part 121 of the Commissioner's Regulations, each district must create a data security and privacy policy by October 1, 2020.[1] To learn more about this requirement, agencies may review Part 121.5 of the Regulations. Use the below table to assist with determining the process you will use as a district to develop this policy by the October 1, 2020 deadline.[1]

KEY QUESTIONS FOR DISTRICT POLICY PROCESS
WHAT IS YOUR DISTRICT'S PROCESS FOR NEW POLICY ADOPTION?
DOES YOUR DISTRICT SUBSCRIBE TO AN EXTERNAL POLICY SERVICE?
HOW MUCH LEAD TIME DOES YOUR BOARD OF EDUCATION (BOE) NEED?
WHO WILL PRESENT THIS POLICY TO, AND HAVE RELATED DISCUSSIONS WITH, YOUR BOE?

[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.

This resource is relevant to the DATA SECURITY AND PRIVACY POLICY Part 121 of the Commissioner's Regulations Requirements.

SOFTWARE INVENTORY RESOURCE

The NIST CSF Core is organized into functions, categories, and subcategories. The first function is "Identify", and the first category within that function is "Asset Management". This category includes the inventory of software platforms. Solutions used at the district, school, and classroom levels must be included in the inventory. As an example, select one software platform used in your district and populate the recommended inventory elements using the table below.

SYSTEM INFORMATION	
SYSTEM NAME	
VENDOR	
SYSTEM TYPE	
DATA INFORMATION	
SCOPE OF IMPLEMENTATION	
TYPE OF DATA	
SYSTEM IMPLEMENTATION AND TERMINATION DATES	
SECURITY AND CONTINUITY PRACTICES	
HOST LOCATION	
BACKUP PRACTICES	
ACCESS CONTROLS	
MAINTENANCE MANGEMENT	
LOG REVIEW	
SECURITY MONITORING	
DATA DESTRUCTION PRACTICES	
CONTRACTUAL PROTECTIONS	
PROCUREMENT METHODOLOGY	
PROTECTIONS ALIGNED WITH FEDERAL AND STATE LAWS	

This resource is relevant to the NIST CYBERSECURITY FRAMEWORK Part 121 of the Commissioner's Regulations Requirements.

THIRD-PARTY CONTRACTS CHECKLIST

Select one district software platform and work with colleagues to populate information from the related contract into the third-party contracts' checklist.

VENDOR: _____ **PRODUCT:** _____

CONTAINS: ☐ **Student Data** ☐ **Teacher or Principal Data**

REVIEW BY: _____ **REVIEWED DATE:** _____

It is highly recommended that the reviewer attach related agreements to this checklist. Use Tables 1 and 2 to populate information related to the statutory requirements that must be addressed in each contract.

CONFIDENTIALITY REQUIREMENTS	2-D	121	Y	N	WHAT SECTION?
Is there a provision that confidentiality of the shared data be maintained in accordance with federal and state law?	5(d)	2(c)			
Is there a provision that confidentiality of the shared data be maintained in accordance with the district/BOCES Policy on Data Security and Privacy?	5(d)	2(c)			

DATA SECURITY AND PRIVACY PLAN REQUIREMENTS	2-D	121	Y	N	WHAT SECTION?
Is there a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the district/BOCES Policy on Data Security and Privacy?	5(e)	6(a)			
Does the plan specify the administrative, operational and technical safeguards and practices the contractor has in place to protect personally identifiable information?		6(a)			
Does the plan demonstrate compliance with the supplemental information requirements (see Table 3)?		6(a)			
Does the plan specify how the vendor's officers and employees who have access to protected data will receive training on the federal and state laws governing confidentiality of the data prior to receiving access?	5(e)	6(a)			
Does the plan specify how the vendor's assignees (subcontractors) who have access to protected data will receive training on the federal and state laws governing confidentiality of the data prior to receiving access?	5(e)	6(a)			
Does the plan specify if the contractor uses subcontractors and how it will manage any relationships and contracts to ensure personally identifiable information is protected?		6(a)			
Does the plan specify how the contractor will manage data security and privacy incidents, identify breaches and unauthorized disclosures, and promptly notify the agency?		6(a)			
Does the plan specify whether, how and when data will be returned to the agency, transitioned to a successor contractor, or destroyed by the contractor when the contract is terminated?		6(a)			
Does the plan include a signed copy of the district/BOCES Parents Bill of Rights for Data Privacy and Security?	5(e)				

THIRD-PARTY CONTRACTS CHECKLIST

Use Table 3 to populate information the district/BOCES needs to post about the contract (supplemental information) with the Bill of Rights for Data Privacy and Security.

SUPPLEMENTAL INFORMATION ELEMENT	2-D 121		SUPPLEMENTAL INFORMATION
The exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract	3(c)	3(c)	
How the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract	3(c)	3(c)	
When the agreement expires and what happens to the protected data when the agreement expires	3(c)	3(c)	
If a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how	3(c)	3(c)	
Where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated	3(c)	3(c)	
How the data will be protected using encryption.	3(c)	3(c)	

THIRD-PARTY CONTRACTS CHECKLIST

Use Table 4 to populate information about other contract considerations relevant to Education Law 2-d and general contractual best practices.

CONTRACT CONSIDERATION	2-D	121	Y	N	WHAT SECTION?
Includes language that requires the vendor to provide notice of breaches and unauthorized disclosures of protected data in accordance with the Commissioner's Regulations (no more than 7 days after discovery).	6(a)	10(a)			
Includes language that tracks the statutory requirements imposed on vendors by Section 2-d, subsection 5(f) and the related regulations:					
• Vendor will adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;		9(a)			
• Vendor will comply with the data security and privacy policy of the district/BOCES, Education Law Section 2-d, and Part 121 of the Commissioner's Regulations;		9(a)			
• Vendor will limit access to education records to persons with a legitimate educational interest;	6(f)	9(a)			
• Vendor will not use education records for any purposes other than those explicitly authorized in the contract;	6(f)	9(a)			
• Vendor will not disclose PII to any other person (except a person authorized by the vendor to help carry out the contract) without consent of the parent or eligible student, unless required to do so by statute or court order and the educational agency has been given notice of the disclosure;	6(f)	9(a)			
• Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII student information;	6(f)	9(a)			
• Vendor will use encryption technology to protect data in motion and data at rest using a technology or methodology specified in guidance issued by the U.S. Secretary of Health and Human Services to implement HIPAA.	6(f)	9(a)			
• Vendor will not sell PII nor use or disclose it for any marketing or commercial purpose, and will not facilitate the use or disclosure of PII by any other party for any marketing or commercial purpose, and will not permit any other party to do so; and		9(a)			
• If Vendor engages a subcontractor to perform its contractual obligations, it shall ensure that the subcontractor is contractually bound to comply with the same data protection obligations imposed on the Vendor by state and federal law and this contract.		9(b)			

The contract is governed by New York State law without regard to the state's choice of law rules, and venue is in the District's county and federal court district.			
Indemnification language is bilateral, not merely requiring the District to indemnify the vendor.			
Price increases capped.			

This resource is relevant to the THIRD-PARTY CONTRACTS Part 121 of the Commissioner's Regulations Requirements.

ANNUAL EMPLOYEE TRAINING PLANNING RESOURCE

As required by Part 121 of the Commissioner's Regulations, agencies must annually provide information privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training should include, but not be limited to, training on the laws that protect personally identifiable information and how employees can comply with such laws. Use the table below to consider the training options. If you decide to include an option in your PD Plan, identify the target audience and date/timeframe in the implementation column.

TITLE	SCOPE	LENGTH	STYLE	IMPLEMENTATION
Cybersecurity Courses	• General Security Awareness • Common Threats	10 Mins - 60 Mins	Online SafeSchools* KnowBe4* GCN*	
FERPA 101 for Local Education Agencies Course	• FERPA Scope and Rights	40 Mins	Online (PTAC)	
Data Protection Reminders for Educators Video	• Data Security and Privacy Best Practices	5 Mins	Video (RIC One Resource)	
Education Law 2-D Overview Course	• Education Law 2-D Requirements for Educational Agencies	75 Mins	Online (RIC One Resource)	
District Specific Policies and Procedures			District Developed	

Individual Responsible for PD Coordination: _____

*These offerings require a subscription.

This resource is relevant to the ANNUAL EMPLOYEE TRAINING Part 121 of the Commissioner's Regulations Requirements.

UNAUTHORIZED DISCLOSURE COMPLAINT FORM

Parents, eligible students (students who are at least 18 years of age or attending a postsecondary institution at any 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. Review and refine the related sample district form and discuss how best to communicate this process to district stakeholders.

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:

This resource is relevant to the UNAUTHORIZED DISCLOSURE COMPLAINT PROCEDURE Part 121 of the Commissioner's Regulations Requirements.

INCIDENT RESPONSE PLANNING RESOURCE

Document the core systems that are essential to your district's operations, communications, and academic-related services. Specify how critical those systems are to district operations in order to prioritize recovery functions. Additionally, note how you plan to continue core district processes in the event of a system loss or extended unavailability.

SYSTEM CATEGORY	CORE SYSTEM	SYSTEM CRITICALITY	CONTINUITY PROCEDURES
COMMUNICATIONS 	Internet		
	Phone		
	Directory Services		
	E-mail		
OPERATIONS 	File Servers		
	Security and Facilities		
	Financial		
	NYSED Business Portal		
STUDENT SAFETY, ACADEMICS AND SERVICES 	Student		
	Transportation		
	Cafeteria		
	Special Education		

This resource is relevant to the INCIDENT REPORTING AND NOTIFICATION Part 121 of the Commissioner's Regulations Requirements.

DATA PROTECTION OFFICER DECISION-MAKING

The chart below outlines steps districts may take related to the appointment of a Data Protection Officer. The shaded steps may or may not be relevant based on decisions made earlier in the process. Check off the tasks as you move through the process with the district leadership team.

CATEGORIES	TASK	COMPLETE
REVIEW FIELD GUIDANCE DOCUMENTATION	Review the NYSED CPO's "Possible Profile of a Part 121 Data Protection Officer" and the RIC One "Data Protection Officer Potential Responsibilities, Qualifications, and Considerations" resources and decide: • which of these duties will be assigned to the District's Data Protection Officer, and • any additional responsibilities that will be assigned to the District's Data Protection Officer.	☐
ANALYZE STAFFING	Review job description or scope of work for District personnel currently performing technologyand student information management duties (e.g., tech coordinator, FERPA student records manager), and • identify which duties are already assigned to existing personnel, and • identify which duties are not currently being performed.	☐
REVIEW RIC SERVICES	Identify whether unassigned duties can be provided by your RIC and review related base and/or optional offerings.	☐
DETERMINE POSITION TYPE	Evaluate whether the District wants a Data Protection Officer with a background as a licensed professional educator (Education Law position), or a non-instructional background (Civil Service Law position).	☐
DETERMINE STAFFING APPROACH	Determine whether the Data Protection Officer responsibilities will be assigned to an existing position or a newly-created position (Education Law or Civil Service Law).	☐
SEEK CIVIL SERVICE SUPPORT, IF NECESSARY	If the District wishes to create a full-time Civil Service Law position, it may be necessary to apply to have your local Civil Service jurisdiction create a Job Specification for the position.	☐
BOARD ACTION, IF EXISTING POSITION	If a title and duties are being assigned to an existing position, the Board of Education should take action to designate the DPO.	☐
BOARD ACTION, IF NEW POSITION	If a new position is being created, Board action should be taken to create the position and then to fill it, after any necessary posting and advertising.	☐

This resource is relevant to the DATA PROTECTION OFFICER Part 121 of the Commissioner's Regulations Requirements.