PART 121
OF THE COMMISSIONER’S REGULATIONS
OVERVIEW RESOURCE

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 SUBMITTED FEEDBACK AND REGULATIONS REFINED
JAN 2019 - DEC 2019

BOARD OF REGENTS ADOPTED THE REGULATIONS
JAN 2020

EDUCATIONAL AGENCIES ADOPT DATA SECURITY AND PRIVACY POLICY
OCT 1, 2020

DEVELOPED BY:
RICone
TWO 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.
## 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, 121.5, 121.7
- **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 the agency’s 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** 121.7
- **Deliver annual privacy and security awareness training to all employees and officers with access to protected data**

### 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**
Education Law Section 2-d and Part 121 of the Commissioner’s Regulations outline requirements for educational agencies and their third-party contractors in order to protect student and annual professional performance review personally identifiable information. Districts need to balance the benefits of using data and the responsibility to minimize the collection of PII in order to reduce risk. Additionally, educational agencies can not sell or disclose PII for commercial purposes. To learn more about protected data, agencies can review Part 121.2, 121.5 and 121.7 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.

<table>
<thead>
<tr>
<th>PERSONALLY IDENTIFIABLE INFORMATION</th>
<th>STUDENT NAME</th>
<th>PARENTS’ NAMES</th>
<th>STUDENT ADDRESS</th>
<th>STUDENT NUMBER</th>
<th>LINKABLE INFORMATION</th>
</tr>
</thead>
</table>

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 (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.

### Data Will Not Be Sold and Will Not Be Released for Commercial Purposes

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

<table>
<thead>
<tr>
<th>Exclusive Purposes for Data Use</th>
<th>Data Accuracy/Correction Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>The exclusive purposes for which the student data [or teacher or principal data] will be used by the third-party contractor include ____.</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subcontractor Oversight Details</th>
<th>Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>This contract has no subcontractors. OR</td>
<td>• The data is stored ______________.</td>
</tr>
<tr>
<td>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 ______________.</td>
<td>• The security protections to ensure data will be protected include ___________.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contract Lifecycle Practices</th>
<th>Encryption Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The agreement expires ________.</td>
<td>Data encryption is applied in accordance with Education Law §2-d.</td>
</tr>
<tr>
<td>• When the agreement expires, the student data [or teacher or principal data] will be __________.</td>
<td></td>
</tr>
</tbody>
</table>

---

**PART 121 OF THE COMMISSIONER’S REGULATIONS | PAGE 3**
Part 121 requires educational agencies to adopt a policy on data security and privacy by October 1, 2020.¹ The chart below highlights some of the components that may 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**

- **NIST CSF ALIGNED PRACTICES**
  - NIST Cybersecurity Framework aligned practices

- **DATA GOVERNANCE**
  - ensure every use of PII benefits students and the educational agency

- **DISCLOSURE AVOIDANCE**
  - protection of PII in public reports

- **STATE AND FEDERAL LAWS**
  - FERPA, IDEA, and other laws

- **DATA PROTECTION OFFICER**
  - employee responsible for the implementation of the policies

- **ANNUAL EMPLOYEE TRAINING**
  - privacy and security awareness training

- **COMPLAINT PROCEDURES**
  - complaints about breaches or unauthorized releases of student data

- **INCIDENT REPORTING AND NOTIFICATION**
  - report the breach to the NYSED CPO and impacted stakeholders

**POLICY IMPLEMENTATION TIMELINE**

- **NYSED MODEL POLICY AVAILABLE**
  - Spring 2020

- **LOCAL MODEL POLICIES AVAILABLE**
  - Spring 2020

- **AGENCY ADOPTS DATA SECURITY AND PRIVACY POLICY**
  - By Oct 1, 2020 ¹

- **POLICY IS POSTED ON WEBSITE AND NOTICE PROVIDED**
  - By Oct 1, 2020 ¹

- **DATA PROTECTION OFFICER MONITORS COMPLIANCE**
  - Ongoing

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.
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.

### 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**

- common desired cybersecurity outcomes (aligned to the Core) are prioritized in a K-12 Target Profile

**CURRENT PROFILE**

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

**GAP ANALYSIS**

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

**ACTION PLAN**

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

<table>
<thead>
<tr>
<th>Data Security and Privacy Plan</th>
<th>Additional Statutory and Regulatory Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Implementation of All Requirements</strong></td>
<td><strong>NIST CSF Safeguards</strong></td>
</tr>
<tr>
<td>Security Protections</td>
<td>Comply with Agency Policy and Law 2-D</td>
</tr>
<tr>
<td>Supplemental Info Compliance</td>
<td>Limit Access to PII</td>
</tr>
<tr>
<td>Contractor Training</td>
<td>Only Use PII as Authorized</td>
</tr>
<tr>
<td>Subcontractor Training</td>
<td>Not Disclose PII to Any Other Party</td>
</tr>
<tr>
<td>Subcontractors Management</td>
<td>Safeguard the PII in Custody</td>
</tr>
<tr>
<td>Cyber Incident Plan</td>
<td>Encryption Practices Applied</td>
</tr>
<tr>
<td>Data Transfer and Disposal</td>
<td>Prohibitions on PII Commercial Use</td>
</tr>
<tr>
<td>Signed Copy of the Bill of Rights</td>
<td>Oversight of Subcontractor</td>
</tr>
</tbody>
</table>

### 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

- [ ] Contractual Obligations
- [ ] Additional Statutory and Regulatory Obligations

---

**Part 121 of the Commissioner’s Regulations | Page 6**
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 121.7 of the Regulations.

### ANNUAL EMPLOYEE TRAINING

#### SUGGESTED PRIVACY AND SECURITY AWARENESS TRAINING TOPICS

<table>
<thead>
<tr>
<th>LAWS, POLICIES, AND PROCEDURES</th>
<th>SECURITY AWARENESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data Security and Privacy Policy</td>
<td>• Common Threats</td>
</tr>
<tr>
<td>• Incident Reporting</td>
<td>• Phishing Recognition</td>
</tr>
<tr>
<td>• Laws and Regulations</td>
<td>• Social Engineering</td>
</tr>
<tr>
<td>• Click Wrap Agreements</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

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

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.
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.

### Unauthorized Disclosure Complaint Procedures

#### Complainant 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

<table>
<thead>
<tr>
<th>Complainant Name</th>
<th>Date Complaint Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description of the Complaint</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date the Finding Report Was Shared with Complainant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
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.

**INCIDENT REPORTING AND NOTIFICATION STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Breach or Unauthorized Release</td>
</tr>
<tr>
<td>2</td>
<td>Incident Response Plan Implemented and Findings Logged</td>
</tr>
<tr>
<td>3</td>
<td>Reported to CPO No More Than 10 Days After Discovery</td>
</tr>
<tr>
<td>4</td>
<td>CPO Investigates Disclosure</td>
</tr>
<tr>
<td>5</td>
<td>If Attributable to a Contractor, Penalties May Be Issued</td>
</tr>
<tr>
<td>6</td>
<td>Agency Notifies Impacted Families and Staff No More Than 60 Days After Discovery</td>
</tr>
</tbody>
</table>

**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.
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.

DATA PROTECTION OFFICER

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