NYS ED LAW 2-D DATA PROTECTION & PLANNING

VERSION DATE: OCTOBER 1, 2020 | **ELECTRONIC VERSION:** https://riconedpss.org/

RIC one

TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE

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.