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

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 to help organizations manage data security and privacy risk. Districts will use a Target Profile, Current Profile, and Action Plan to apply these activities. To learn more about this requirement, review Part 121.5 of the Regulations.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

COMPLIANCE CHECKS

Policy:

- ✓ Aligns with the NIST CSF
- ✓ Is Adopted by October 1, 2020

Action Plan:

- ✓ Identifies Priority Action Items to Address Profile Gaps

NIST CSF VERSION 1.1 OVERVIEW

FRAMEWORK CORE
A set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors

FRAMEWORK CORE FUNCTIONS
The Core consists of five concurrent and continuous functions—Identify, Protect, Detect, Respond, Recover. These functions provide a high-level, strategic view of the organization's management of cybersecurity risk.

FRAMEWORK IMPLEMENTATION TIERS
Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

FRAMEWORK PROFILE
The Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories

CURRENT PROFILE AND TARGET PROFILE
Profiles are used to identify opportunities for improving the cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).

ACTION PLAN
The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks.

IDENTIFY, ASSESS, & MANAGE CYBER RISKS

NIST CSF CORE & PROFILE ACTION PLANNING DIAGRAMS

The Core is a set of desired cybersecurity activities organized into 5 functions, 23 categories, and 108 subcategories. Profiles, aligned to the Core, are used to identify opportunities for improving the cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).