# 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).