NYSED DATA SECURITY REVIEW

NYSED Information Security Office is implementing a data security review with LEAs beginning in the first quarter of 2024. NYSED has identified several foundational focus areas for LEAs to implement working towards a stronger data security posture. The areas identified below align with elements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and feature some of the key tactics, activities, and guidelines (also known as controls) suggested by NIST to address the review areas NYSED will focus on.

Below is a reference guide for the areas we will review with you and your team, within this guide there is also the NIST CSF subcategory reference.

POLICIES	CONTROLS	THIRD-PARTY
• Acceptable Use • Disaster Recovery • Incident Response • Incident Response Plan • Password • Privacy and Security	• Access Control (i.e., Physical and Electronically) • MFA • Password Complexity • Patch Management • Users On/Off Boarding Process	• Type of Data Shared • How Data is Shared • Where Data is Stored • Encryption in Transit/Stored • Access Controls on Data Sets • Third-Party Environment Configurations

LEGEND:
CSF Subcategory: These are subcategories outlined in the NIST CSF* that the LEA can use as a resource to address any areas they are deficient in or wish to improve their posture in the category.

Primary/Applicable Subcategory Controls: These are subcategories are outlined in the NIST SP 800-53 Rev. 5 that LEAs can use as a resource.

**Note: CSF 1.1 used for this model*

1. **REVIEW PASSWORD MANAGEMENT.**
   a. CSF Subcategory(s): PR.AC-1, PR.AC-6, PR.AC-7
   b. PRIMARY/APPLICABLE Subcategory Controls: IA-1, IA-2, IA-5
2. **REVIEW HOW DATA IS SHARED WITH THIRD-PARTY CONTRACTORS.**
   a. CSF Subcategory: ID.SC-3 PRIMARY/APPLICABLE Subcategory Controls: SA-4, SA-9, SR-2, SR-3
   Ed Law 2-d Requirements, Part 121:
   b. 121.2: AC-21, AT-3(5), AU-2, PT-2, PT-3, PM-5(1), SA-8(33), SI-12(1)
   c. 121.3: PM-20, PT-5,
3. **DISCUSS MFA IMPLEMENTATION.**
   a. CSF Subcategory: PR.AC-1, PR.AC-7
   b. PRIMARY/APPLICABLE Subcategory Controls: AC-14, IA-1, IA-2
4. **REVIEW POLICY FOR ONBOARDING AND OFFBOARDING ACCOUNTS.**
   a. CSF Subcategory: PR.AC-1, PR.AC-4
   b. PRIMARY/APPLICABLE Subcategory Controls: AC-1, AC-2, AC-5, AC-6, IA-1, IA-2, IA-5
5. **REVIEW CURRENT POLICIES, SUCH AS: ACCEPTABLE USE, PASSWORD, INCIDENT RESPONSE, DISASTER RECOVERY AND PRIVACY AND SECURITY.**
   a. CSF Subcategory: ID.GV-1, ID.GV-3
   b. PRIMARY/APPLICABLE Subcategory Controls: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1
6. **DISCUSS ASSET INVENTORY AND THE ABILITY TO IDENTIFY CRITICAL ASSETS.**
   a. CSF Subcategory: ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5
   b. PRIMARY/APPLICABLE Subcategory Controls: CA-3, CM-8, CP-2, PM-5, RA-2, RA-9

IKON EDUTECH GROUP