



CHIEF PRIVACY OFFICER
(518) 474-0937
E-mail: privacy@nysed.gov

CHIEF INFORMATION SECURITY OFFICER
(518) 486-4940
E-mail: infosec@nysed.gov

TO: All New York State School Data Protection Officers

FROM: Louise DeCandia, Chief Privacy Officer and
Marlowe Cochran, Chief Information Security Officer

DATE: May 1, 2023

RE: Remaining Vigilant

As May approaches and the 2022-2023 school year starts to wind down, the New York State Education Department's Chief Privacy Officer and Chief Information Security Officer ask you to remain vigilant about maintaining your school's cyber hygiene.

As you are all aware, cyberattacks on schools throughout the nation and New York continue. *Indeed, the bottom line is that your school district is a target.* Please ensure that your districts and schools continue to work towards the National Institute of Science and Technology (NIST) Cybersecurity Framework and consider these best practices and requirements to reduce your districts' risk:

- 1) **Multi-Factor Authentication.** If you haven't already, please implement Multi-Factor- Authentication (MFA) before t

caught. It can slow down attackers and reduce their impact. Review who gets administrative rights.

- 6) **Password Policy.** Please implement a password policy that bans common words and requires no less than 14 characters. This, in addition to MFA can help ensure that staff, students, and threat actors do not get unauthorized access to confidential data.
- 7) **Phishing Simulations.** Phishing simulations are activities designed to train employees to recognize, avoid, and report potential threats. Managed simulations should be used to track responses and provide targeted training for employees.
- 8) **Incident Response Plan.** All districts should have a Cyber Incident Response Plan that details how your district responds to a cyber event. It should set forth roles and responsibilities and be regularly reviewed and practiced by leaders throughout the district.
- 9) **Network Access Management.** Continuously review and assess the devices that access the district networks.
- 10) **Training.** As required by Education Law Section 2-d and Commissioner's regulation §121.7.
- 11) **MS-ISAC Membership.** If you are not a member of the MS-ISAC, please consider [joining](#). It provides valuable information on threats, vulnerabilities and free remediation tools.

THANK YOU for your dedicated and continued work protecting New York's schools' data.

CISA Cyber Hygiene Services - Routine Vulnerability Scanning and Services from CISA

- x <https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services>

NYS Cyber Reporting - DHSES CIRT – Incident Response Support

- x Technical Response Assistance
- x 1-844-OCT-CIRT

NYS Intelligence Centers Cyber Analysis Unit – NYS cyber distribution lists with cyber advisories and alerts

- x Join today by contacting: cau@nysic.ny.gov