

CHIEF PRIVACY OFFICER'S ANNUAL REPORT
ON DATA PRIVACY AND SECURITY

Pursuant to Education Law § 2-d, the New York State Education Department's (NYSED) Chief Privacy Officer is required to issue an annual report on:

- (1) Data privacy and security activities and progress,
- (2) The number and disposition of reported breaches, if any, and
- (3) A summary of any complaints of possible breaches of student data or teacher or principal annual professional performance review (APPR) data.

This report addresses the reporting period of January 1 to December 31, 2022.

- I. Opening and Summary of Data Privacy and Security Activities and Progress

Part 121 of the Commissioner's regulations,

- A staff member's email account credentials were compromised under unknown circumstances, which resulted in unauthorized logins from an unidentified IP address located out-of-state.
- A student's student information management system account was compromised when a classmate watched the student enter his credentials. The classmate thereafter accessed the account and sent inappropriate emails.
- A malicious actor pretending to be a representative of an employment website gained access to the Microsoft 365 accounts of a student and a staff member. The actor thereafter used these accounts for phishing purposes.

-
- At three educational agencies, a video surveillance system (Intralogic) became infected with Malware.
 - At one educational agency, staff checked a server after hours and identified a shell command that had failed. The educational agency contacted Homeland Security, installed appropriate patches, manually checked its file system, and installed cybersecurity software as a further precaution.
 - At one educational agency, permission misconfigurations by a student management system allowed teachers outside of the district to access a small number of student assignments.
 - At one educational agency, it was believed that bad actors were staging a ransomware attack by accessing a student's virtual desktop by logging into their student account. There was no evidence to support that any student PII was accessed.
 - It is believed that Black Cat Ransomware encrypted and locked down two servers at one educational agency; no PII was compromised.
 - A staff member's payroll and bank account information were imperiled when the staff member provided their Microsoft account credentials in response to a phishing email. The unauthorized user was unable to access the staff member's Microsoft account due to multifactor authentication; however, the unauthorized user accessed payroll and bank information as the staff member used the same credentials for that account.

- A school administrator prepared spreadsheets with PII to share with individuals outside of the school district for the purpose of seeking student participation in youth sports.
- A teaching assistant was discovered taking and selling photos of students to companies that license stock photos as part of an outside business.
- A teacher sent the names, school identification numbers, and dates of birth of her

Article 1315 (1)(d) of the Education Law and Section 121.10 of the Regulations of the Commissioner of Education

III. Disposition of Data Incident Report Filings

End Section 87(2)(b) of the Education Law and Section 121.10 of the Regulations of the Commissioner of Education

Education Law § 87(2)(b) and Section 121.10 of the Regulations of the Commissioner of Education require educational agencies to report every discovery (o)10 8.7473 63.912 557.65449([-73

V. Investigations and Dispositions of Complaints

Section 121.4 of the regulations of the Commissioner of Education and NYSED's § 2-d Bill of Rights for Data Privacy and Security