THE SCHOOL DISTRICT OF PHILADELPHIA

No. 830

Section: 800 Operations

Title: Cyber Incident Response

Adopted: May 18, 2017

Revised: January 30, 2025

830 CYBER INCIDENT RESPONSE

Purpose

As a custodian of sensitive data belonging to students, employees, and parents, the Board of Education ("Board") recognizes its responsibility to safeguard this data from unauthorized use, disclosure, disruption, modification, or destruction. While data loss or compromises may not be completely preventable, the Board enacts this Policy to promote confidentiality, integrity, and availability of the information assets owned and operated by the School District of Philadelphia ("District"). This Policy directs the District to establish a framework for responding to cyber security incidents in a timely and structured fashion that balances the need for transparency with ongoing privacy, cybersecurity, and legal considerations.

Authority

As authorized by the Pennsylvania Public School Code, the Board may adopt and enforce such reasonable rules and regulations as it may deem necessary and proper regarding the management of its school affairs. [1]

Furthermore, as required by the Pennsylvania Breach of Personal Information Notification Act, the District shall provide notice of any breach of the security of its data systems in conformity with that Act. [2]

The Board therefore requires that records containing personal information be securely maintained, stored and managed in compliance with state and federal laws, regulations, Board policy, and administrative regulations.

Delegation of Responsibility

The Board directs the Superintendent or their designee, through the Office of Information Technology and Data Management (OITDM), to develop Administrative Procedures and other protocols that outline how the District will plan to respond to cyber security incidents, such as breaches of personal information maintained by the District.

OITDM shall develop these Administrative Procedures and protocols to take into account industry best practices, including any necessary training.

OITDM shall outline the plan for training of the District's Incident Response team, as defined in the Administrative Procedures to this Policy.

OITDM shall report on the information security strategy and implementation periodically to the Superintendent and the Board.

OITDM, upon a determination of a breach in the security system, shall provide notice to the district attorney in the county where the breach occurred and to any resident of the Commonwealth whose unencrypted and unredacted personal information OITDM has determined was or is reasonably believe to have been subject to unauthorized access. Notification will be in accordance with Administrative Procedures and as required by law.[2]

The Board emphasizes the shared responsibility of all District employees, students, and those with access to District systems to follow the protocols developed relating to the Policy, as well as those related to the District's Information Security Policy. [3]

Legal References:

1. 24 P.S. § 5-510
2. 73 P.S. 2301 et seq
3. Policy 829 - Information Security