THE SCHOOL DISTRICT OF PHILADELPHIA

Effective: January 30, 2025

Administrative Procedures for Cyber Incident Response
(Attachment for Policy No. 830)

Purpose

The purpose of the Cyber Incident Response Administrative Procedures are to describe the protocols that the School District of Philadelphia (District) will develop as guidelines and steps that it will take when it responds to actual threats to the integrity of its technology operations and/or data, including necessary and suggested steps regarding investigation, communication, containment, and recovery efforts.

Definitions

Cybersecurity Event
An event is an exception to the normal operation of IT infrastructure, systems or third-party services. Events may be identified through the use of automated systems; reported violations to the ISO, Compliance/Privacy or other District department; or in the course of normal system reviews including system degradation/outage. It is important to note that not all events become incidents.

Cybersecurity Incident
An incident is an event that, as assessed by OIT staff, violates the Acceptable Use Policy, Access Control Policy or other District policy, standard, or Code of Conduct or threatens the confidentiality, integrity, or availability of Information Systems or Data.

Regulated Data Classification
Regulated Data may have additional reporting and regulatory requirements when dealing with incidents.

Procedures

The District is committed to a reasonably rapid and holistic response to cybersecurity events or incidents that threaten the District's operations or security of District data.

The Incident Response process encompasses six phases that the District's Incident Response Team will focus on, including preparation, detection, containment, investigation, remediation and recovery. The District shall develop a private, confidential Protocol that will not be available for

public access for each of these areas and they are described as follows and based on the National Institute of Standards and Technology (NIST) framework:

- **Preparation:** Preparation for incident response includes those activities that enable the organization to respond to an incident and include the creation and review of policies; annual training and review of protocols; standards and guidelines supporting incident response; security and technology related tools; effective communication plans and governance; thresholds for reporting. Preparation also implies that the organizations across the District have implemented the controls necessary to enable the containment and investigation of an incident. As preparation happens outside the official incident process, process improvements from prior incidents should form the basis for continuous improvement at this stage.
- **Detection:** Detection is the identification of an event or incident whether through automated means with security tools or notification by an inside or outside source about a suspected incident. This phase includes the declaration and initial classification of the event/incident.
- **Containment:** Containment of an incident includes the identification of affected hosts, systems or location and their isolation or mitigation of the immediate threat. Communication with affected parties is established at this phase of incident response.
- **Investigation:** Investigation is the phase where ERT personnel determine the priority, scope, risk and root cause of the incident.
- **Remediation:** Remediation includes the repair of affected locations, systems and services, addressing residual attack vectors against other systems, communication and instructions to affected parties and an analysis that confirms the threat has been contained. Malware or other unauthorized access should be removed and cleaned during this stage.
- **Recovery:** Recovery is the analysis of the incident for possible procedural and policy implications. Recovery also includes the incorporation of any “lessons-learned” from the handling of the incident into future exercises and/or training initiatives.

If the Deputy CISO believes that an exposure of regulated data may have occurred that meets the defined threshold outlined in the Preparation Protocol mentioned above, then the Deputy CISO will contact the General Counsel and, in turn, they will contact the Chief of Staff to provide situational information and convene the Incident Response Team.

If the thresholds for the Deputy CISO to report the incident to the General Counsel and Chief of Staff have been met, then any formal investigative reports or after-action analysis will be completed at the direction of the General Counsel, or the engaged outside counsel.

The following Roles and Responsibilities are expected to be involved throughout the course of responding to a cybersecurity event or incident.

- (Deputy) Chief Information Security Officer:
    - Coordinating efforts to manage an cyber security incident;
    - Ensuring the prompt investigation of a cyber incident;
    - Directing the prompt reporting of a cyber security incident to law enforcement;
    - Determining what District data may have been exposed;
    - Securing any compromised systems to prevent further damage; and
    - Providing technological guidance to the institutional stakeholders.
- Office of General Counsel:
    - Office of General Counsel to assist in addressing regulatory requirements and notifications, both internally and externally.
- Incident Response Team:
    - The Incident Response Team (IRT) consists of District Officials with the authority to make key decisions in managing an incident. The IRT shall be comprised of the following standing members or offices (note: other members may be asked to collaborate where appropriate):
        - Deputy CISO
        - General Counsel, or designee with license to practice law
        - Chief of Staff
        - Chief of Communications and Customer Service
        - Chief Financial Officer and representative from the Office of Risk Management
        - Chief of School Safety, or designee
        - Chief Operating Officer, or designee
        - Chief, Director, or Department Head of the area where the exposure is determined to have occurred (Assistant Superintendent or Principal if occurred at school)
        - Other key employees or representatives/officials as determined by the above officials, depending on the factual scenario.
- Incident Response Coordinator:
    - Appointed by Deputy CISO and may be a representative of the District procured by contract
    - Directing efforts to gather appropriate information
    - Providing expertise in the procedural aspects of gathering information and documentation of process
    - Updating leadership as necessary
- Incident Response Handler:
    - Appointed by Deputy CISO and may be a representative of the District procured by contract

- Gathering data from systems
- Providing specific expertise in technology and data
- Entering appropriate data for Incident Management including procedural information