Administrative Procedures for Information Security
(Attachment for Policy No. 829)

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 can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be completely preventable, the purpose of Policy 829 and its Administrative Procedures is to promote confidentiality, integrity, and availability of the information assets owned and operated by the School District of Philadelphia ("District"). These Administrative Procedures and the protocols linked within establish a framework for risk management in the information security arena and sets the strategic and operational security activities in-line with business objectives.

Definitions

The following definitions apply to these Administrative Procedures and all individual protocols linked within:

Confidentiality: The assurance that information resources are only accessible to those authorized to have access and is protected throughout its lifecycle.

Integrity: The safeguarding of the accuracy and completeness of information and the processing methods that are applied to a given piece of information or data set.

Availability: The guarantee that authorized users have access to information and IT services when required.

Information Asset: Any data, information, or IT service, in any format, that the District owns or manages for which the District is responsible. This can include software, hardware, data, intellectual property, and personal information.

Information Systems: The IT infrastructure, networks, and applications enabling the processing, transfer, and storage of information used as a part of the District's core operations.

National Institute of Standards and Technology (NIST): Agency of the United States Department of Commerce whose mission promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.

NIST Cybersecurity Framework: A security and policy framework of computer security guidance for how organizations can assess and improve their ability to identify, protect, detect, respond, and recover from cyber attacks.

Cybersecurity Risk: The potential that a given threat might exploit a vulnerability associated with an asset or group of assets, resulting in harm to the organization.

Unauthorized Access: Any access to District information or information assets that has not been explicitly approved by the appropriate authority (e.g., person, team, etc.).

Non-Compliance: Failure to act in accordance with a stated rule, regulation, or policy.

Procedures

The District is committed to managing security risk to information assets across five domains: Identify; Protect; Detect; Respond; Recover. Under each domain, the Office of Information Technology and Data Management (OITDM) maintains protocols that take into account industry best practices.

Many of these protocols are available to the public and linked below. However, due to security risks associated with publicizing the District's entire information security plan, several protocols remain confidential and accessible only to designated OITDM staff. Publicly accessible protocols include details about providing training to users of District information assets and systems, where applicable.

Information Security Protocols

I. *Identify*
   A. Software Use: Sets forth the rules for the use of software on systems within the District's information technology environment.
   B. Vulnerability Management (Internal & Confidential): Defines the process for identifying, evaluating, treating, and reporting vulnerabilities on systems within the District's information technology environment.
   C. Risk Management (Internal & Confidential): Establishes a framework for identifying, assessing, mitigating, and monitoring risks associated with the use, processing, storage, and transmission of information within the District's systems and networks.
   D. Change Management (Internal & Confidential): To establish a controlled and coordinated approach for managing changes to the District's information systems and technology environment, to minimize the potential negative impact on services, data, and users.
   E. Monitoring and Reporting (Internal & Confidential): To establish guidelines for the monitoring of network and system activities and for reporting any suspicious or unauthorized activities across the District's information systems and networks.
   F. Identification and Authentication (Internal & Confidential): To establish requirements for identifying and authenticating users who seek access to the District's information systems and data, assessing whether each user is appropriately identified and validated before access is granted.

G. Supply Chain Risk Management (Internal & Confidential): To manage and mitigate the risks associated with the District's reliance on suppliers, vendors, and third parties. This Protocol aims to establish structure for the District to manage these relationships in a way that they do not introduce unacceptable risk into the District's operations or compromise the security of its data and systems.

II. Protect

A. Security Awareness and Training: Provides all individuals within the District who have access to information systems with the necessary awareness, knowledge, and skills to protect these systems and the associated data.
B. Equipment Disposal: Outlines the responsibilities and procedures for the disposal of District-owned equipment, including computing and electronic devices, to prevent sensitive data from being exposed and to outline how to dispose of equipment in an environmentally responsible manner.
C. Information Technology Planning: Establishes a structured, strategic approach to the planning and implementation of information technology (IT) initiatives and budgeting within the District.
D. Network and Systems Access: Defines requirements for and control user access to the District's network and systems
E. Network and Wireless Security (Internal & Confidential): To establish guidelines for securing the District's network and wireless services, protecting them from unauthorized access, disruption, or misuse, and ensuring the confidentiality, integrity, and availability of information. This is inclusive of networks within the schools and administrative buildings across the District.
F. Systems Security (Internal & Confidential): To provide guidelines for managing the security of the District's information systems, providing guidance on security controls that protect these systems against unauthorized access, disruption, modification, or destruction.
G. Email Security (Internal & Confidential): To define the security standards for systems used to send, receive, and store email across the District. This Protocol aims to protect the District's information systems and data from threats delivered by or associated with email, including spam, phishing, and malware.
H. Encryption and Data Protection (Internal & Confidential): To provide guidelines for the proper handling, storage, and transmission of sensitive data using encryption and other data protection methods to help prevent unauthorized access or disclosure.
I. Physical and Environmental Protection (Internal & Confidential): To establish measures to physically protect the District's information resources. This Protocol aims to support the security, availability, and integrity of these resources by mitigating threats from physical and environmental factors and resources located within physical property owned or leased by the District.

J. System Maintenance (Internal & Confidential): To establish a framework for the consistent, effective maintenance of the District's IT systems. This Protocol aims to set a standard that systems remain secure, reliable, and efficient in supporting the District's operations and objectives.
K. Mobile Device Access (Internal & Confidential):To establish rules for the use of mobile devices, including smartphones and tablets, to access, store, transmit, or receive District resources or data. This Protocol aims to reduce the risks, such as data loss or unauthorized access, that arise from the use of mobile devices.

III. Detect

A. Data Accountability: Defines the rules for creating, protecting, and retaining information system audit records to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities.
B. Cloud Services Security (Internal & Confidential): To provide guidance on the secure use of cloud services within the District, including how data is stored, accessed, shared, and protected in the cloud.
C. Application Security Development Lifecycle (Internal & Confidential): To support application services being developed within the District with a firm security foundation. This Protocol focuses on managing the risk of software applications developed and maintained by the District within their pre-production and operational environments.

IV. Respond

V. Recover

A. Information Processing and Release: Guides the secure handling, processing, and release of information within the District, with a particular focus on how information is handled when it may be released to the public.
B. Backup and Recovery (Internal & Confidential): To define the steps necessary to maintain data backups and support the District's ability to recover data in the event of a loss. This Protocol is intended to protect the School District's data assets and the availability thereof.

Maintenance Schedule

These Administrative Procedures and the protocols designated within shall be reviewed upon the review of the Policy, or upon the occurrence of a triggering event.

Related Information:

NIST Cybersecurity Framework