

December 18, 2025


**AUTHORIZE THE COMMENCEMENT OF THE PUBLIC COMMENT PERIOD FOR THE
INFORMATION SECURITY POLICY**

THE INTERIM SUPERINTENDENT/CHIEF EXECUTIVE OFFICER RECOMMENDS:


That the Board authorize the commencement of the Public Comment Period from December 19, 2025, to January 19, 2026, for the Policy described in the disposition table below. Pursuant to Board Bylaws Rule 1-2 VI (B), the Board must authorize the commencement of the Public Comment Period.

Current Policy Section/ Current Policy Title	New Policy Section/ New Policy Title	Description of Revision/Disposition
Board Report 13-0925-PO1 Information Security Policy		The purpose of this policy is to authorize the Chief Information Officer, the Executive Director of Information Security, or Designee to develop, establish and implement District-wide information privacy and security measures using the NIST (National Institute of Standards and Technology) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations and other state-of-the-art standards, guidance and protocols relevant to the unique information private and security concerns of educational institutions.

Approved as to Legal Form: Initial
LB

Signed by:

 974F0DEB7385497...
Elizabeth K. Barton
Acting General Counsel

Approved:

Signed by:

 1406F92741F44F8...
Macqueline King, Ed.D
Interim Superintendent/Chief Executive Officer

AMEND BOARD REPORT 13-0925-PO1
INFORMATION SECURITY POLICY

THE CHIEF EXECUTIVE OFFICER RECOMMENDS:

That the Board of Education ("Board") amend Board Report 13-0925-PO1 Information Security Policy.

PURPOSE: The purpose of this policy is to authorize the Chief Information Officer, ~~and~~ the Executive Director of Information Security, or Designee to develop, establish and implement District-wide information privacy and security measures using the *NIST (National Institute of Standards and Technology) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations* and other state-of-the-art standards, guidance and protocols relevant to the unique information private and security concerns of educational institutions in order to:

- (1) protect the confidential information maintained in District's data, systems, and electronic records from unauthorized disclosure including, but not limited to, student and employee information, operational plans, and financial information
- (2) protect against security breaches and system attacks while allowing business processes to function on a continuous, uninterrupted basis with reasonable assurance that the data and information has not been altered
- (3) protect against the misuse or improper use of the District's information resources to a level that protects the Board while still allowing day-to-day functions.

POLICY TEXT:

I. Definitions

CIPA: The Children's Internet Protection Act (CIPA) is a U.S. law that requires schools and libraries to use internet filters and implement online safety policies to protect children from harmful online content.

CJIS: The Criminal Justice Information Services (CJIS) Security Policy is a set of federal guidelines that govern how criminal justice agencies and their partners protect sensitive law enforcement information.

COPPA: The Children's Online Privacy Protection Act (COPPA) is a U.S. law that protects the privacy of children under 13 by regulating how websites and online services collect, use, and share their personal information.

NIST Cybersecurity Framework (CSF): The NIST Cybersecurity Framework (CSF) is a set of guidelines and best practices that helps organizations identify, protect against, detect, respond to, and recover from cyber threats. It's important because following it ensures compliance with government regulations, strengthens security, and builds trust by keeping systems and data safe.

Zero trust architecture: a cybersecurity approach that requires continuous verification of every user, device, and request, granting only minimal access and never assuming trust.

II. Security and Privacy Controls

The Chief Information Officer ("CIO"), ~~and~~ the Executive Director of Information Security (EDIS), or Designee shall assess the District's systems threats and vulnerabilities and develop, establish and implement appropriate control measures to protect electronic data and information resources commensurate to the risk of adverse events. The CIO, ~~and~~ EDIS, or Designee shall develop, establish and revise as necessary District-wide standards, requirements, procedures and control measures using NIST 800-53 NIST Cybersecurity Framework (CSF), COPPA, CIPA, CJIS, and other contemporary industry standards, guidance and protocols relevant to the unique needs of educational institutions, specifically in the following areas:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Asset Monitoring and Tracking
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- Component Authenticity
- System and Communications Protection
- Port and I/O Device Access
- System and Information Integrity
- Zero trust architecture
- Remote learning/EdTech controls
- Accountability via KPIs/metrics
- Vendor Risk
- Artificial Intelligence Use and Oversight
- Cloud Security
- Bring Your Own Device

The control measures established by the CIO, ~~DIS~~ EDIS, or Designee should address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance with applicable federal and state data privacy and security laws, and procedures to facilitate the implementation. The CIO, EDIS, or Designee shall issue additional implementation guidance, standards, and procedures for each control area to support alignment with instructional technology needs, remote learning systems, mobile device usage, and other educational applications.

III. Responsibilities

The Chief Information Officer ("CIO"), Executive Director of Information Security (EDIS), or Designee shall maintain overall responsibility for the establishment, oversight, and enforcement of the District's Information Security Program. The CIO, EDIS, or Designee shall coordinate efforts across CPS departments and schools to ensure compliance with this Policy, supporting standards, and applicable federal and state laws and regulations.

All CPS employees, contractors, and authorized users are responsible for protecting District information and information systems in accordance with this Policy and related standards. School and department leadership shall support implementation efforts, promote awareness, and ensure alignment with instructional and operational needs. The CIO, EDIS, or Designee shall periodically review and update responsibilities in response to organizational, legal, and technological changes.

IV. Violations

Failure to abide by this Policy or standards, guidelines, procedures or control measures issued by the CIO, ~~or DIS~~ EDIS, or Designee will subject employees or students to discipline up to and including dismissal in accordance with Board Rules and Policies. Any Board contractor, consultant, or other business partner who violates this policy may have their system access privileges suspended and may be further subject to contract termination or any other remedy or action deemed appropriate by the Board.