Chicago Public Schools Policy Manual

Title: **INFORMATION SECURITY POLICY**
Section: **102.7**
Board Report: 13-0925-PO1 **Date Adopted:** September 25, 2013

Policy:

THE CHIEF EXECUTIVE OFFICER RECOMMENDS:

That the Board rescind Board Report 04-0825-PO3 adopt a new Information Security Policy.

PURPOSE: The purpose of this policy is to adopt the *NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations* as the standard for implementing District-wide security measures in order to: (1) protect the confidential information maintained in the 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 District's data and information has not been altered; and (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:

A. Security and Privacy Controls

The Chief Information Officer ("CIO") shall assess the District's systems threats and vulnerabilities and implement NIST 800-53 control measures to protect electronic data and information resources and minimize the risk of adverse events. The CIO shall develop, establish and revise as necessary, standards, requirements, procedures and control measures to implement NIST 800-53 District-wide in at least 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

The NIST 800-53 control measures established by the CIO 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.

B. Violations

Failure to abide by this Policy or related NIST 800-53 standards, guidelines, procedures or control measures issued by the CIO will subject employees to discipline up to and including dismissal in accordance with Board Rules and Policies.

Amends/Rescinds: Rescinds 04-0825-PO3 (Adopted September 22, 2004)
Cross References:
Legal References: