

DEFERRED

ADOPT A NEW INFORMATION SECURITY POLICY

THE CHIEF EXECUTIVE OFFICER RECOMMENDS:

That the Chicago Board of Education ("Board") adopt a new Information Security Policy.

~~PURPOSE: The purpose of this policy is to establish a single, unified information security standard that~~

will protect all District data, systems and electronic records. By establishing information security

1.3 OTHER RELEVANT POLICIES

The following is a list of other Board policies pertaining to information security that are managed and maintained by OTS.

1.3.1 Member Acceptable Usage Policy, Board Report #04-0428-PO2, as may be amended from time to time.

1.3.2 Student Acceptable Usage Policy, Board Report #03-0326-PO03, as may be amended from time to time.

1.4 DEFINITIONS OF TERMS

1.4.1 USER

Users, as defined in this policy, include all Board employees, students, contractors, consultants, temporaries, and other computer users at CPS, including those users affiliated with third parties who use Board equipment and/or access CPS data or systems.

1.4.2 SERVER

A Server is defined as any computing system that is owned and/or administered by CPS which provides services to users. Examples include, but are not limited to: email systems, web servers, video conferencing devices, and file/print servers.

1.4.3 SYSTEM ADMINISTRATOR

A System Administrator is defined as any Board employee, contractor, consultant, temporary, or other person who administers and/or manages the administration of

2.0 USER ACCOUNTS AND ACCESS PRIVILEGES

2.1 DIRECTORY SERVICES

2.1.1 All access-level user accounts and access credentials (for use by general users of a system or application) shall be created and maintained via enterprise directory services maintained by OTS.

2.1.2 Creation of separate pools of user accounts for local servers, applications, or services must be approved by OTS management.

2.2 ACCOUNT AUTHORIZATION

2.2.1 All user access accounts must be created by a process that ensures user ID

validity and security.

2.2.2 Accounts for users who are not Board employees must be authorized by a

2.4.3 All passwords, including local account passwords, shall be changed on a

regularly scheduled basis.

2.4.4 OTS shall perform regular system audits to verify password compliance.

3.0 NETWORK SECURITY

3.1 NETWORK SECURITY ARCHITECTURE

3.1.1 OTS managed servers must be separated from client networks by a firewall (or

4.1.3. All servers must have all security patches and fixes applied in a timely manner

4.1.4 All servers must have OTS standard software installed, including, but not limited to, remote management and anti-virus software.

4.1.5 All servers must have OTS management accounts installed with administrative

rights to the machine.

4.1.6 All devices must have local authentication preventing unrestricted access. Local accounts and/or console access must be password protected. Local access accounts must adhere to security policy regarding user account, including password complexity requirements.

4.1.7 All OTS managed servers must be located in approved data centers or approved and maintained equipment closets/rooms (usually referred to as MDF rooms)

5.0.4 All workstations must prevent unrestricted access; this is primarily implemented

via a login process combined with a password protected screen saver set to engage in a reasonable amount of time.

5.0.5 All local accounts must be password protected with passwords that adhere to

password complexity requirements.

7.0 DATA SECURITY AND APPLICATION SECURITY

7.1 DATA CLASSIFICATION

~~All data processed, stored, and disseminated within ODS shall be categorized according~~

to sensitivity levels established by OTS.

7.2 DATA SECURITY

7.2.1 Applications that store confidential and restricted data must reside on equipment in a data-tier that is separated by a firewall (or equivalent traffic filtering). Equipment

housing this data shall not be directly accessible by end users.

7.2.2 It is understood and accepted that sensitive data will always exist in a transient fashion across the network on access-tier equipment such as application servers, web browsers, and/or client applications; however, permanent, semi-permanent, and/or per

7.4 DATA USAGE

All users shall ensure that their duties and activities have the following accessibilities according to:

use of Board data.

7.4.1 PERTINENT USE OF DATA

Board information shall be only used to conduct Board business. Using internal data for personal use or for professional use unrelated to Board business is forbidden.

7.4.2 PRIVACY AND CONFIDENTIALITY OF DATA

All users shall ensure the confidentiality of data they work with. Users are expected to respect control measures used to protect confidential and restricted data and not to circumvent these measures.

7.4.3 ACCURACY OF DATA

Effort shall be made to ensure data is kept in an accurate state. Users shall not

9.1.3 CONTRACTORS, CONSULTANTS, AND OTHER BUSINESS PARTNERS

Any Board contractor, consultant, or other business partner who violates this policy may

have their system access privileges suspended and may further be subject to contract termination or any other remedial action deemed appropriate by the Board.

9.2 RESPONSIBILITY AND ACCOUNTABILITY

9.2.1 USERS

All individuals described in the scope section of this document are responsible and accountable for complying with the data security tenets detailed in this policy and are liable for their violation. This includes responsibility and accountability for user accounts and access to information entrusted to them by the Board and for insuring the privacy of