

ADMINISTRATIVE 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. It establishes 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 #02-0226-PO02, as may be

## 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

services maintained by OTS.

2.1.2 Creation of separate pools of user accounts for local servers, applications, or

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 equivalent traffic filtering). Exceptions must be approved by OTS information security management.

3.1.2 Networks shall be separated into security network zones such that all student computers are separate from administrative computers (defined as Instructional and Administrative networks).

3.1.3 Network traffic shall be subject to content filtering in accordance with government regulations. There are no exceptions to this requirement.

3.1.4 Where technically feasible, equipment shall have an appropriate "terms of use" banner displayed to those persons accessing the system or device.

**3.2 NETWORK SECURITY POLICY**

network security zones. Exceptions are made for school-managed servers, which shall be restricted by service type.

3.1.6 Internet accessible systems and services shall be built as security-hardened

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.

5.0.6 Workstations shall display a "Terms of Use" banner to those persons accessing the

system.

## 6.0 REMOTE ACCESS

This section covers the use of remote access technologies such as dial-up, Virtual Private Networking (VPN), and remote control applications.

### 6.1 USER REQUIREMENTS

6.1.1 The purpose of remote access is to allow remote users to access Board computing

**7.0 DATA SECURITY AND APPLICATION SECURITY**

**7.1 DATA CLASSIFICATION**

All data generated, stored, and disseminated within ODC 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.

**7.4 DATA USAGE**

All users, regardless of other duties and position, have the following responsibilities regarding the 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 misrepresent data.

**8.0 MONITORING AND POLICING**

**8.1 MONITORING**

8.1.1 QTS has the right to inspect, monitor, and log any and all aspects of its



9.1.3 CONTRACTORS, CONSULTANTS, AND OTHER BUSINESS PARTNERS

have their system access privileges suspended and may further be subject to contract termination or any other remedy or 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 access, credentials, and data used by the Board. Individuals may be held liable for the misuse