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 standards, the Board can reduce liability risks, ensure data confidentiality, and maintain information systems integrity.

SCOPE: This policy applies to all Board employees, students, contractors, consultants, temporaries, and other computer users at the Chicago Public Schools ("CPS"), including those users affiliated with third parties who access Board data and/or systems. This policy applies to all computer and communication systems connected to the Board network that are owned by and/or administered by the Board or its designees and the operation of these systems.

POLICY TEXT:

1.0 INTRODUCTION, GOALS, DEFINITIONS

1.1 GOALS

The three main goals for this information security policy are data confidentiality, system integrity and risk management as further described below.

DATA CONFIDENTIALITY

The Board maintains vast amounts of personal, financial and operational data stored on information systems and used by staff for daily operations. Much of this data is sensitive in nature, and its misuse may violate state and federal regulations. The primary goal of CPS information security is the protection of all confidential information including student information.

SYSTEM INTEGRITY

CPS relies on its Information Technology ("IT") infrastructure to conduct day-to-day business. With student information processing, payroll, financial systems, building facilities, and phone/fax services all running on one network infrastructure, any impact to the network's availability may halt the entire enterprise. Any force that affects the availability of the IT infrastructure is a force that acts against CPS operations. Therefore, this policy will also protect against security breaches and system attacks and to allow business processes to function on a continuous, uninterrupted basis.

RISK MANAGEMENT

With the increased level of interconnectedness provided by modern IT systems, there is an increased risk of individuals misusing Board network resources. Risks include, but are not limited to: email accounts being used to falsely represent the Board to other agencies or entities; unauthorized release or access to sensitive data; attacks on other systems being launched from Board networks, either by internal users or outsiders who have gained access to Board networks; and the use of file sharing programs from the Board network in violation of copyright laws.

1.2 POLICY IMPLEMENTATION

The Office of Technology Services ("OTS") is responsible for overseeing the implementation, management and maintenance of this policy.

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 computer and communication systems owned by and/or administered by the Board.

1.4.4 NETWORK

A Network is defined as a logical area containing the virtual presence of a collection of electronic systems.

1.4.5 MANAGEMENT (OF A DEVICE) BY OTS

Management of a piece of equipment includes administration by any OTS employee, assigned contractor, consultant or other temporary employee designated by OTS.

1.4.6 BOARD-DESIGNATED MANAGER

Board-designated managers include Principals and CPS Department Heads or their designee.

1.4.7 NETWORKS: ADMINISTRATIVE, INSTRUCTIONAL

The Board network is divided into network security zones. The two primary zones are the Administrative and Instructional networks. The Administrative network is used for all business related functions; the Instructional network is allocated to student education functions. Additional network security zones may be defined by OTS.

1.4.8 TERMS OF USE BANNER

A message that is displayed by a system to a user in order to notify them that they are accessing a Board system. This message must state a minimum of the following: that unauthorized use is prohibited, that the user agrees to basic terms such as acceptance of this policy and other Board policies, and that they will be held liable for unauthorized access, violation of policy, and misuse of the system.

1.5 STANDARDS, GUIDELINES, AND PROCEDURES

OTS shall issue information security standards, guidelines, and procedures that will effectuate this policy. All Users shall comply with such OTS standards, guidelines, and procedures.

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 Board-designated manager. This authorization may be in the form of an approval of a procedure or business process for the granting of access.

2.2.3 Remote access accounts must be individually approved by a Board-designated manager.

2.2.4 Security controls shall not be circumvented in order to escalate account privileges or to create accounts not otherwise approved through the appropriate processes.

2.3 USER ACCOUNT REQUIREMENTS

2.3.1 Shared accounts are strictly forbidden with the exception of local system administration accounts.

2.3.2 Guest access accounts are not allowed unless specifically approved by OTS Management. Guest access accounts are accounts on system and applications that provide a basic level of access with minimal or no authentication for outside users.

2.3.3 Where appropriate, systems shall be engineered to disable or delete accounts that are inactive for an excessive period of time.

2.3.4 Computer labs will often utilize a generic account for authenticating workstations. These accounts shall have restricted access levels should only allow access to the systems in that lab. Lab accounts are still accountable to password complexity rules. Care must be taken to not advertise these accounts.

2.4 PASSWORDS

2.4.1 All passwords are considered restricted data and shall not be shared with others, openly displayed, or otherwise be allowed to be known by others. Users are responsible and accountable for user accounts and access credentials entrusted to them by the Board.

2.4.2 All passwords, including those for local, application, and system administration accounts are required to conform to password complexity rules; systems should be built to enforce this behavior via system policy.

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.

3.1.5 Internet accessible services on the Board network shall be restricted to specific 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 "bastion" hosts. Firewall rules permitting access are conditional to system security; these rules may be disabled or revoked if the internal server is found to be vulnerable or compromised.

3.2 WIRELESS SECURITY

Best effort shall be made to keep wireless networks secure and closed to the outside. In order to fulfill this requirement, the following standards are required by policy.

3.2.1 All wireless network traffic must be encrypted.

3.2.2 Open wireless access points that do not prevent unauthorized access are strictly forbidden.

3.2.3 All wireless network equipment must meet OTS standards.

3.2.4 Wireless network equipment shall not be placed outside the Instructional network unless expressly permitted by OTS.

4.0 SERVER SECURITY

4.1 ALL SERVERS

This section applies to all server equipment owned and/or operated by the Board.

4.1.1 All servers not managed by schools must be managed by OTS.

4.1.2 All servers must be actively maintained by administrators. The purchase and installation of any server assumes that provisions are made to maintain the server in a secure manner.

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).

4.1.8 All servers must be registered within OTS. At a minimum, the following information is required:

- Server contact(s), including backup contact(s)
- Network hostname and IP address
- Operating system type and version
- Primary functions and applications

4.1.9 Servers shall display an appropriate "terms of use" banner to those persons accessing the system.

4.2 OTS-MANAGED SERVERS

This section is specific to servers managed by OTS.

4.2.1 All servers must be built and maintained according to OTS standards.

4.2.2 All test, development, and other non-production servers must be located in OTS datacenters and must meet the required standards.

4.3 SCHOOL-MANAGED SERVERS

This section is specific to school-managed servers.

4.3.1 All school-managed servers must have OTS management accounts installed with administrative rights to the machine.

4.3.2 All servers must follow all other standards as defined by OTS.

5.0 WORKSTATION SECURITY

All workstations connected to Board networks must be maintained and secured.

5.0.1 All workstations must have all security patches and fixes applied in a timely manner.

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

5.0.3 All workstations must have OTS management accounts installed with administrative rights to the machine.

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 and information resources within the Board network. Access for personal or private business use is not allowed. Using remote access for the purpose of connecting to the Internet for non-business functions is not allowed.

6.1.2 Users must abide by all terms of the Board's Acceptable Use Policies while using their remote access connection.

6.2 RESTRICTIONS

6.2.1 Remote access to interior systems is restricted to explicitly defined resources and is subject to approval by OTS.

6.2.2 Remote control applications cannot be used without tunneling them through Board approved VPN services. Direct connections to or from the Internet for the purpose of controlling internal devices from outside the Board network are not allowed; these connections must be conducted through VPN services and are subject to approval by OTS.

6.2.3 Direct dial remote control is only allowed for the purpose of system administration and should have proper security controls in place. Dial-up to user workstations is prohibited.

6.3 END SYSTEM REQUIREMENTS

It is expected that workstations used for remote access be properly secured.

6.3.1 Workstations located within the Board network must meet workstation requirements as described in Section 5.0 of this policy.

6.3.2 OTS is unable to support remote workstations (outside the Board network), and requires the end user to adequately guard their personal workstations against security hazards. This includes ensuring the workstation has up-to-date anti-virus software and has all security patches applied on a regular basis.

6.4 ACCOUNT EXPIRATION

Any remote access account not used for 180 consecutive days will be terminated.

7.0 DATA SECURITY AND APPLICATION SECURITY

7.1 DATA CLASSIFICATION

All data processed, stored, and disseminated within CPS 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 non-volatile storage of sensitive data must abide by security policy. Any exceptions must be approved by OTS senior management.

7.2.3 All applications that house confidential or restricted data will be subject to regular audits by an OTS-authorized auditor.

7.3 APPLICATION SECURITY

This section applies to applications that access Board data which are developed for the Board via outside agencies or internal developers.

7.3.1 All applications must be built so that data security is designed into the system.

7.3.2 User accounts and authentication for applications shall be tied to the Board directory services architecture.

7.3.3 All applications developed for or by the Board shall have third party security audits as part of their budgeted operation. Successful passing of a third party audit shall be part of any contract for such an application.

7.3.4 Applications that provide varying levels of access to Board data are required to have stringent access controls with clear and consistent access policies for users. Access control should be role-based and tied to the Board directory services.

7.3.5 The business owners of an application (those who are the primary owners of the data and processes that the application supports) shall maintain a data classification report that lists the mapping of users (or groups) who have access to data.

7.3.6 Application systems which house confidential or restricted data shall be built or modified to have mechanisms that provide monitoring and logging functions in order to detect and log inappropriate access or access attempts to confidential or restricted data.

7.3.7 All effort shall be made to ensure that confidential and restricted data is encrypted and remains encrypted when stored and transmitted by an application.

7.3.8 Where applicable, applications shall display a "terms of use" banner to users accessing the system.

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 OTS has the right to inspect, monitor, and log any and all aspects of its information systems in order to execute the tenets of this policy, including, but not limited to, systems connected to the CPS network, data residing on computing systems and data in traffic traveling across the CPS network.

8.1.2 OTS shall monitor the network and systems to detect anomalous behavior and investigate such behavior when observed. This behavior may include, but is not limited to: policy violations, system attacks, peer-to-peer traffic, and virus/trojan/worm activity.

8.1.3 OTS has the right to examine any aspect of the environment in order to investigate and correct information security events. OTS reserves the right to access and make changes to any system connected to the CPS network (regardless of ownership of that system) to address security concerns. OTS reserves the right to deny access to any system to address security concerns.

8.2 AUDITING

CPS shall perform audits of its environment in order to complete security assessments. These audits include, but are not limited to: password audits, penetrations tests, system (workstation and server) assessments, and application audits. All such audits will be conducted by either an OTS-authorized auditor or an Audit Department-authorized auditor.

9.0 POLICY VIOLATION, RESPONSIBILITY AND ACCOUNTABILITY

9.1 POLICY VIOLATION

9.1.1 EMPLOYEES

Employees who violate this policy may have their system access privileges suspended and may further be subject to disciplinary action in accordance with the Board's Employee Discipline Rules and Policies.

9.1.2 STUDENTS

Students who violate this policy may have their system access privileges suspended and may further be subject to disciplinary action in accordance with the Board's Student Uniform Discipline Code.

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 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. Users may be held liable for the misuse of their Board-assigned access credentials or user accounts by others who gain access to their credentials.

9.2.2 IT GOVERNANCE COUNCIL
The IT Governance Council is responsible and accountable for ensuring that proper oversight and support of data security requirements is uniformly applied across the District.

9.2.3 SCHOOLS
For school-owned and/or operated equipment, services, and data, principals and their designees are responsible and accountable for executing the tenets of this and other Board data security policies and standards.

9.2.4 BOARD-DESIGNATED MANAGERS
Board-designated managers are required to exercise discretion in granting access privileges to users. Board-designated managers will approve access to non-Board users only when necessary and required to perform critical functions. Board-designated managers may share responsibility for the actions taken by users for whom they have authorized accounts and/or resource access. Board-designated managers are responsible for overseeing and executing the relevant data security tenets in the manner required by their job function.

9.2.5 OFFICE OF TECHNOLOGY SERVICES
OTS is responsible and accountable for developing, implementing, coordinating, and policing practices in accordance with this policy.

Approved For Consideration:

Barbara Eason-Watkins
Chief Education Officer

Approved:

Arne Duncan
Chief Executive Officer

Noted:

John Maiorca
Chief Financial Officer

Approved as to Legal Form:

Ruth Moscovitch
General Counsel