
**The Office of
The Chief Technology Officer**

Computer Systems Security Procedures

**Version 3.1
Working Document**

(Intentionally left blank)

Table of Contents

1.0	Introduction.....	5
2.0	Security Awareness Procedures.....	5
3.0	Electronic Data Security.....	6
3.1	Managing User Identification.....	6
3.1.1	User Account Provisioning	6
3.2	Managing Passwords	8
3.2.1	User Password Creation	8
3.2.2	Entering Passwords	9
3.2.3	Safeguarding Passwords.....	10
3.2.4	Safeguarding System Administrators' Password	10
3.3	Logging In to the System.....	10
3.4	Defining Levels of Access.....	11
3.5	Copying and Printing Information.....	11
3.6	Backing Up Data	11
3.6.1	System Administrators' Responsibilities	12
3.6.2	End Users' Responsibilities	12
3.7	Electronic Signatures.....	12
3.8	Data Sanitation	12
4.0	Physical Security	13
4.1	Environmental Requirements	14
4.2	Accessing Work Areas	14
4.3	Moving Computer Equipment	15
4.4	Using Personally Owned Computers or peripherals.....	16
4.5	Securing Central Data Center	16
4.6	Preventing Damage and Recovering Data.....	17
5.0	Systems and Applications Security.....	18
5.1	Application Code Vulnerabilities	18
5.2	Security of Web-based Applications	20
6.0	Telecommunications Security	21
6.1	Wide Area Network/Local Area Network (WAN/LAN)	21
6.2	Internet Use	21
6.2.1	Electronic Mail (E-mail)	23
6.2.2	Electronic Mail (E-mail) Retention.....	24
6.3	Remote Access	24
6.3.1	Security Considerations.....	25
6.3.2	Teleworking	25
6.4	Protecting MCPS Assigned Computing Equipment.....	26
6.5	Surveillance Cameras (CCTV).....	26
7.0	Investigations.....	26
8.0	E-Discovery.....	26
8.1	Notice of claim	26

9.0 Noncompliance 26
Appendix: Abbreviations 29

1.0 Introduction

The Information Assurance and Risk Management (IARM) unit under the direction of the the Chief Technology Officer (CTO) is responsible for establishing and maintaining systemwide information security practices, standards, guidelines, and procedures. This manual provides guidance, direction, and authority for information security in Montgomery County Public Schools (MCPS) and is in alignment with the MCPS Board of Education's Regulation IGT-RA, *User Responsibilities for Computer Systems, Electronic Information, and Network Security*.

This manual provides guidance and contains information specific to staff responsible for supporting the district's technology systems. This includes, but is not limited to, IARM unit members, school- and nonschool-based information technology systems specialists (ITSS), program developers, network administrators, and other technical staff. In particular, this manual includes security requirements for the following:

- Security awareness
- Electronic data security
- Physical environment and personal computers
- Systems and applications
- Telecommunications

This document is reviewed annually and updated as needed to reflect the evolving nature of MCPS practices and standards, as well as to address new and emerging threats. Updates will be distributed as changes are made.

2.0 Security Awareness Procedures

Staff and students are responsible for safeguarding computers and electronic information. Staff from the Office of the Chief Technology Officer (OCTO) will coordinate and provide security awareness information to staff and students as follows:

- IARM staff will be available to provide security awareness and proper computer use presentations to staff and students throughout each school year.
- Staff and students will receive a copy of the CyberSafety brochure.
- OCTO staff will develop and make available the IT (Information Technology) Security Awareness brochure.
- A CyberSafety website will be available to staff and students.
- New teachers will be provided with the computer security awareness information.
- ITSS staff will receive security awareness updates during regularly scheduled meetings.
- Staff will receive security awareness alerts as security risks are identified and warranted.
- IARM staff will coordinate with the Technology Consulting Team to incorporate IT security awareness in technology-related trainings.

3.0 Electronic Data Security

This section describes the security requirements for electronic data, including user identifications (ID) and passwords, access, backups, copying, and electronic signatures. Users are required to enter positive identification to access MCPS electronic data.

3.1 Managing User Identification

All users must have their identity verified through a unique user ID and a confidential password, or other means that provides equal or greater security, to gain access to MCPS multi-user computers and networked computers or communication system resources. User IDs are assigned by staff in OCTO upon authorization.

3.1.1 User Account Provisioning

Network, e-mail, and all other system IDs are assigned by established procedures for students and staff. The student identification number assigned upon enrollment in MCPS serves as the student's user ID. Employee IDs are assigned centrally using the MCPS Employee Login Table (MELT) ID process. All other IDs for special situations are assigned by local network administrators upon approval by the authorized administrator or designee.

Accounts are to be modified, disabled, or removed when a user's status is changed. Changes to the Human Resources Information System initiate the process for changing, deleting, or disabling accounts. The local system administrator is responsible for ensuring that proper access is monitored and maintained.

Staff user accounts may be immediately disabled by OCTO staff at the direction of the Office of Human Resources, the CTO, or a designee.

The following table displays the convention for assigning user IDs to access MCPS resources.

User	Login ID	Password	Comments
Pre-kindergarten– Second Grade	Graduation year and student ID number	No passwords	Time limited between 8:00 a.m. and 4:30 p.m.
Third-Fifth Grades	Graduation year and student ID number	Six-character passwords made by combining two 3-character words	Time limited between 8:00 a.m. and 4:30 p.m.
Middle Schools	Graduation year and student ID number	Six-character passwords made by random generation	Time limited between 7:00 a.m. and 5:00 p.m.
High Schools	Graduation year and student ID number	Six-character passwords made by random generation	Time limited between 7:00 a.m. and 5:00 p.m.

Parent Teacher Association (PTA) Members	School number, PTA, and first and last initial (for example, 652PTALW)	Eight-character passwords made by random generation	Time limited between 7:00 a.m. and 5:00 p.m. Account ends at the end of the school year.
Long-term Substitutes	Current standards as staff teachers, as provided by the MELT table	Eight-character passwords made by random generation	Current standards as staff teachers.
Short-term Substitutes	Outlook username and login	Outlook username and login	Provided with an account that only has access to Outlook.
Health and Human Services – Health Services	Current standards	Current standards	Current standards as staff teachers.
Interagency Coordinating Board	See appropriate category above	See appropriate category above	Student accounts can be extended beyond the day with prior approval by the principal.
Staff without a MELT ID (new hire staff)	School number and TMP01-TMP35 (For example: 652TMP01)	Password assigned for each new hire by designated staff	Time limited between 7:00 a.m. and 5:00 p.m.
Training Accounts	School number and TRN01-TRN35 (for example: 652TRN01)	Password assigned for each training session	Time limited between 7:00 a.m. and 8:00 p.m. Accounts are disabled after training session is completed.
Nonschool-based Office (NSBO) Staff	Melt-ID	Eight-character password	Current standards

Students—MCPS has a process in place to update and validate students at the beginning of each school year. New student accounts are created, as required, by the ITSS at the enrolling/receiving school. Any special requests by parents to limit student access are addressed on a case-by-case basis. All special requests must be resubmitted each year.

School staff—The ITSS, principal, or their designee may identify a staff person to administer account access. All ID and permission rights must be validated and verified.

Central office staff—a supervisor, director, or their designee may identify a staff person to administer account access. All ID and permission rights must be validated and verified annually or when a position change occurs.

Non-MCPS staff or students—MCPS does not provide access to its protected systems except for an approved educational purpose. Special exception requests must be made to the appropriate administrative authority. An MCPS staff member must identify the user and state the educational purpose. Examples include the following:

- Application systems and network—Contract service providers may receive access. The department contracting the service must identify the provider in a memorandum, signed by the individual and the sponsoring office/department designee. Access is not permitted for general community members.
- E-mail for community members—Restricted to individuals with a specific project relationship who are nominated and approved by the Office of Communications and Family Outreach.
- E-mail for MCPS retirees—All MCPS retiree e-mail account requests must be submitted to the e-mail administrator using MCPS Form 271-4A, *Request for an MCPS E-mail Account* for approval. The accounts are valid for one year. Renewal notifications are sent every year to the individual and must be approved by the sponsoring senior administrator or the account will be disabled.
- Specific programs—Contract service providers may be given temporary access for the duration of a work order. The office/department contracting the service must identify contractors. In cases where this involves confidential student, staff, or MCPS information, written confidentiality agreements must be in place.

Users may only access information and computer systems to which they are authorized and that they need for their assignments and responsibilities. Users are responsible for their own individual accounts and are expressly prohibited from sharing accounts and passwords. Users should become familiar with the procedures as outlined in Regulation IGT-RA, *User Responsibilities for Computer Systems, Electronic Information, and Network Security*.

3.2 Managing Passwords

Staff passwords are required to have a minimum of eight characters and contain one upper case and one numeric character. Exceptions to the password creation conventions are stated in section 3.1 as it relates to Kindergarten through Grade 12 students and special situations. All network account holders are required to change their passwords at least once every 120 days, as of February 2010.

3.2.1 User Password Creation

Users create their own passwords based on the following guidelines:

- Users must choose passwords that should be difficult for an unauthorized party to guess. This means that passwords must not be related to a user's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used.
- Recommendations for choosing a password that is easy to remember, but difficult for unauthorized parties to guess are to
 - String together several words into a password phrase.

- Bump characters in a word a certain number of letters up or down the alphabet.
 - Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word.
 - Combine punctuation or numbers with a regular word.
 - Create acronyms from words in a song, a poem, or another known sequence of words.
 - Deliberately misspell a word.
 - Combine a number of personal facts like birth dates and favorite colors.
- Users must not construct passwords that are identical or similar to passwords they have previously employed.
 - Users must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must not employ passwords like “X34JAN” in January and “X34FEB” in February.
 - All system administrators will have unique administrator accounts for administrative purposes only. System administrator accounts are never to be shared with anyone.

3.2.2 Entering Passwords

The number of consecutive attempts to enter a password correctly must be limited. This limitation is to prevent password-guessing attacks. After five unsuccessful attempts to enter a password, the system will temporarily disable the user ID for 15 minutes.

The internal process of the password system for system administrators includes the following features:

- Passwords are never to be displayed near a workstation. When entering, passwords must not be displayed in readable form.
- Passwords distributed via mail, pony, or other physical distribution system are sent separately from user IDs. In addition, passwords should be mailed within an opaque envelope that would readily reveal tampering. The most secure and recommended method to distribute passwords is for the ITSS, system administrator, Help Desk, or designee to personally deliver this confidential information to the user. Passwords for new staff are distributed to the user’s personal e-mail address.
- Passwords are not to be stored in readable form in batch files, automatic login scripts (including e-mail systems), software macros, or terminal function keys in computers without access control, or in other locations where unauthorized persons might discover them.
- Passwords always are to be encrypted when held in storage for any significant period of time or when transmitted over networks. The purpose of this encryption is to prevent passwords from being disclosed to wire-tappers, technical staff reading systems logs, and other unauthorized parties.

- Passwords never are to be hard-coded or incorporated into software developed by or modified by MCPS staff. Hard-coding of passwords does not allow users to change them as needed.
- Computer and communication systems are to be designed, tested, and controlled to prevent the retrieval of encrypted or unencrypted passwords that are stored electronically.
- Passwords for computer and communication system access control must be unique for each user. Anonymous access is strictly unauthorized.
- Passwords supplied by a vendor as a default are to be changed before any computer or communications system is used for MCPS business.

3.2.3 Safeguarding Passwords

Users have the following responsibilities related to their passwords:

- Passwords must not be written down and left in a place where unauthorized persons might discover them.
- Aside from initial password assignment and password-reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password must be changed immediately.
- Passwords must never be shared. As an authorized user, you are responsible for any inappropriate or illegal actions that another party takes while using your password. If you need to share non-confidential computer resident data, use e-mail or public directories on local area network servers.

3.2.4 Safeguarding System Administrators' Password

System administrators have the following password-related responsibilities:

- A multi-user or generic login is strictly unauthorized. Immediately change system or administrator passwords that have been compromised on any computer systems.
- Passwords are not to be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in data communications software, in web browsers, on hard drives, or in other locations where unauthorized persons might discover them.
- Change all appropriate passwords if an unauthorized party has compromised the system or there is a suspicion of compromise. Identify the extent of the compromise. If needed, reload a trusted version of the operating system and all security-related software. Review all recent changes to user and system privileges for unauthorized modifications.
- Obtain picture ID, teacher and supervisor confirmation, partial Social Security Number, or employee ID number before distributing passwords to individuals new to MCPS.

3.3 Logging into the System

The login process for computers must include a banner stating that the system is only for use by authorized users; and by continuing to use the system, the user verifies that authorization.

Specific information must not be displayed on the login screen until a user has successfully provided their user ID and password. The network operating system information should not be displayed.

After a maximum of 60 minutes of computer, terminal, or workstation inactivity, the security or operating system must automatically blank the screen and end the session. Only after, the user has provided their user ID and password will the session be re-established.

Users are not to leave their computer, workstation, or terminal unattended without first logging out or otherwise securing the computer. This is particularly important if the established user session is capable of accessing confidential, sensitive, or valuable information.

3.4 Defining Levels of Access

The computer and communications system privileges are restricted to the authorized users of each office, department, division, or school. Specific written procedures defined within applications and systems outline the level of access that users will be given to various types of information. Program managers are responsible for ensuring that this process is followed. Before accessing confidential information, individuals not employed by MCPS must sign a non-disclosure agreement.

Employees are authorized to view only confidential or personal information according to their job, project, or assigned duties. User privileges will be defined so that end users are unable to gain access to, or interfere with, individual activities or the private data of other users.

Employees with access to confidential information will have restricted access to that information. Employees will take appropriate steps to ensure that confidential materials are not released to unauthorized parties. See EGI-RA, *Release of Information on Students and Employees*; KBB, *Release of Data*; and IGT-RA, *User Responsibilities for Computer Systems, Electronic Information, and Network Security*.

File access control permissions for all MCPS networked systems are set to a default that blocks access by unauthorized users. Users are not to read, modify, delete, or copy a file that belongs to another user without obtaining permission from the owner of the file or appropriate supervisory staff. The ability to read, modify, delete, or copy a file that belongs to another user does not imply permission to actually perform these activities unless general user access is clearly provided.

3.5 Copying and Printing Information

Employees will monitor printers while printing confidential information and will not send confidential information to a printer where unauthorized persons have access.

3.6 Backing Up Data

All MCPS servers are to be regularly backed up onto electronic media.

3.6.1 System Administrators' Responsibilities

The ITSS or system administrator is responsible for the information and must ensure that regularly scheduled backups occur.

System administrators have the following responsibilities for backing up data:

- Regularly test data media that is used for archival storage. The computer data media that is used to store sensitive, critical, or valuable information must be of high quality and periodically tested to ensure that it can record information properly.
- Encrypt or otherwise secure all sensitive, valuable, or critical information that is recorded on backup computer media, such as magnetic tapes, optical disks, and other media stored outside of MCPS offices. This encryption is to prevent the information from being revealed to or used by unauthorized parties.
- Rotate backed up data to off-site storage weekly.

3.6.2 End Users' Responsibilities

Before taking portable computers/laptops off the network, end-users are responsible for backing up and storing their data in a safe place. Data must be backed up for recovery in case the portable computer is lost, stolen, or compromised.

3.7 Electronic Signatures

The process for the use of electronic signature for electronic records transactions must be in compliance with MCPS Board of Education regulations IGT-RA, *User Responsibilities of Computer Systems, Electronic Information, and Network Security*; DJA-RA, *Procurement of Equipment, Supplies, and Contractual Services*; DLB-RA, *Authorized Signatures for Payroll Documents*, Maryland state law, and Federal law.

- Only individuals having a letter from the superintendent or his designee are authorized to have a digital signature for procurement and payroll.
- Digitized electronic signatures must be stored in a secure location and accessible only by authorized personnel or processes as approved by the superintendent or his designee.
- The individual who releases a batch approval of MCPS documents for procurement or payroll using the electronic signature is responsible for the truth and accuracy of everything in the Approval and Certification Statement with respect to each document and transaction in the batch.
- Any user of MCPS computer systems should report suspicious or inappropriate use of data, computer system abuse, or possible breaches of security. School-based users should alert the principal or the principal's designee responsible for information technology. Nonschool-based users should alert their immediate supervisors and the superintendent and/or his designee.

3.8 Data Sanitation

The data sanitation process for system hard drives, backup drives, mobile devices, flash drives, and all other data storage media is as follows:.

- Computers reused by MCPS—Machines are to be reimaged with the proper school image and reinstalled by MCPS staff (or contractual staff) in schools and offices.
- Classroom computers leaving MCPS—These computers are to have no user data on the machine. Machines are removed from the network while still part of the domain. All workstation policies remain in effect. Windows will not permit login with an administrator password. The receiving organization must pull the BIOS/CMOS jumper and set the machine to boot from compact disc (CD). They then must reimage the machine.
- Special education computers—These computers may contain user data from programs such as Woodcock-Johnson, WIATT, and other testing programs. These machines are identified by schools prior to Technology Modernization integration. They are labeled and sent to the recycling warehouse where they are erased using KillDisk.
- NSBO computers—These are computers removed from nonschool-based offices. These are not classroom or school computers. Some user data are likely to be on the local hard drive. The integration team will back up the data onto the user's network drive (home directory) and then erase the machine using KillDisk.
- Functional laptops—All laptops, school and office, are considered to contain user data. All functional laptops are erased using KillDisk prior to being removed from MCPS.
- Dead laptops—When a laptop is returned to the recycling warehouse in a non-functional condition, the drive is removed from the device and erased using a magnetic media device. MCPS currently uses the Verity Systems model V91 media degausser for this purpose. This method destroys the data as well as the hard drive motor.
- Windows file servers—Windows file servers are erased using both Windows utilities and Darik's Boot and Nuke. In the event that drives cannot be erased using this process, the drives are physically removed from the server and erased using the degausser.
- Backup tapes and magnetic media—Used and outdated backup tapes and magnetic media are returned to the recycling warehouse. Magnetic media are erased using the bulk degausser.
- Optical backup media—Optical backup media is shredded by each school, office, or file server administrator.
- Macintosh computers and servers Operating System Extension (OSX)—Hard drives are erased using Macintosh OSX utilities and then have the original operating system reinstalled on the drive.
- Palm Operating System (OS) devices—Palm OS devices are erased and reset to original factory settings prior to disposal. If the Palm OS device will not power-on using either the battery or a power supply, the device is destroyed using a hammer.

4.0 Physical Security

This section describes the security of the physical environment where computers and servers reside. Procedures cover the environmental requirements, accessing work areas, moving

equipment, using personally owned computers, securing the central data center, and preventing damage and recovering data.

There must be the ability to enforce all information systems security controls before they become standard operating procedure.

4.1 Environmental Requirements

Environmental requirements and recommendations are in place to ensure that service continues for critical computer systems. Fire detection and suppression, and power and air conditioning are examples of the computer environmental protection and safety systems. The following steps should be followed:

- Equip areas with critical computer equipment with fire and smoke alarms and fire extinguishers.
- Store critical equipment in a location that minimizes or prevents water damage due to leaking or flooding.
- Anchor tall and top-heavy items to prevent tipping.
- Ensure that items on wheels have locking mechanisms to prevent rolling.

Maintain all equipment in a clean environment that meets or exceeds the manufacturers' specifications related to temperature and humidity. Equipment areas should be free of obstructions. Regularly monitor the cleanliness, environmental protection, and safety systems. Qualified personnel should schedule periodic inspections.

Provide electrical protection. All microcomputers must have surge suppressors. Qualified OCTO personnel must approve these items. All electrical wiring must meet state and local building codes.

Regularly scheduled preventive maintenance on computer and communications equipment should be performed. Preventive maintenance as defined by the manufacturer will help ensure that the risk of failure is minimized.

4.2 Accessing Work Areas

Access to all buildings, classrooms, computer labs, offices, video surveillance and work areas containing computer-related equipment must be physically restricted and controlled. Access to servers and wiring closets must be restricted. Only authorized personnel should have access to wire closets and server areas. Authorized persons may include:

- Authorized OCTO staff
- ITSSs
- Outside contractors hired by MCPS to work in these areas
- Building services and office staff at locations trained to reset equipment

Areas with computer equipment must be locked, where feasible. Access to computer equipment must be supervised. Authorized personnel must be on site when an outside group uses computer

equipment. For nonschool-based offices, use of equipment is authorized by the directors of the Department of Infrastructure and Operations and the Division of Technology Support when MCPS staff is not present.

Access to offices, computer rooms, and work areas containing sensitive information must be physically restricted. Managers who are responsible for employees who work in these locations must determine the appropriate access controls. Employees must not attempt to enter restricted MCPS areas without authorization to do so.

All multi-user computer and communications equipment such as file servers, labs, and wiring closets must be located in secured rooms to prevent unauthorized usage.

4.3 Moving Computer Equipment

Computer or related equipment may not be removed from MCPS property without appropriate authorization by the principal, supervisor, or director of the department owning the equipment. Permission to remove computers or related equipment may be granted only for accepted educational or MCPS business purposes. Equipment that is removed for repairs has implied permission when MCPS-approved repair processes are followed and a receipt is retained for the equipment.

A school or office owning portable computers or related equipment must employ a tracking system to record when computers are loaned out and when they are returned. The tracking system should include the name of the borrower and identification of the computer equipment, along with the date borrowed, and the anticipated length of the loan. Laptops or other portable computer equipment must be returned before personnel transfer to another work location or terminate their MCPS employment.

Microcomputer equipment must not be moved or relocated without prior authorization from the appropriate onsite or designated OCTO staff. Microcomputer workstations, printers, peripherals, file servers, and electronics are examples of microcomputer equipment covered by this requirement. Movement of equipment applies to all permanent and temporary moves. Authorization must be in writing if the equipment will be removed from MCPS property. "Mobile" equipment, such as laptops and equipment mounted on rolling carts, should have a sign-out log to track the movement.

Employees, consultants, or contractors must return all MCPS property when they terminate their relationship with MCPS or with a specific work location within MCPS. The supervisor is responsible for collecting all MCPS property from an employee leaving the assigned work location. Personnel terminating MCPS employment or moving from one work location to another must inform their supervisor or administrator regarding any MCPS property that they have and building access privileges.

When a computer support employee is involuntarily terminated, all MCPS equipment and data should be retrieved immediately. Network accounts for terminated employees should be disabled immediately.

4.4 Using Personally Owned Computers or Peripherals

Employees and students may not bring their own computers or peripherals into the work place without prior authorization. MCPS is not responsible for maintenance, damage, or loss of personally owned computers or peripherals in the work place. Users are not to install or attach personal computers or peripherals to any equipment owned by MCPS without prior authorization from the designated technical support staff or system administrator.

MCPS computer equipment is not to be altered or enhanced in any way without prior authorization from the supervisor and technical support staff, or system administrator.

4.5 Securing Central Data Center

The location of the MCPS central data center is confidential and must not be disclosed without a demonstrated need to know. No signs are to indicate the location of the central data center. Access to the central data center is restricted. Only employees whose job responsibilities require access to the central data center should be granted access. Authorized access is granted through use of the form, *Request for Pass Card*, available from the supervisor of the central data center. The chief technology officer (CTO) must approve any exceptions for access. Anyone who is not authorized to enter the MCPS-secured central data center must be escorted by the central data center supervisor or designee. Tours of major computer and communications facilities must be approved by the central data center supervisor.

Access to magnetic tape, disk, and documentation libraries is restricted to employees whose responsibilities require access. The magnetic tape, disk, and documentation libraries housed within the controlled areas of the central server center require additional precautions. This access is controlled by the supervisor of the central data center.

There must be a secure intermediate holding area for computer supplies, equipment, and other deliveries. Delivery personnel must not have direct access to rooms containing multi-user computer facilities.

The central data center must be equipped with fire doors and other doors resistant to forcible entry. Additionally, the central data center must have automatic, closing doors that are able to set off an audible alarm when left open beyond a designated time period. Firewalls surrounding computer facilities must be non-combustible and able to resist fire for at least one hour. All openings to these walls, such as doors and ventilation ducts, should be self-closing and capable of staying that way for at least one hour.

Employees are not to permit unknown or unauthorized persons to enter restricted areas as they enter and exit these areas. Physical access controls for MCPS buildings are intended to restrict the entry of unauthorized persons, and employees are expected to help restrict such access. When doors to the central data center are propped open for any reason, a central data center employee or designee must monitor the entrance.

4.6 Preventing Damage and Recovering Data

Disaster prevention and recovery should include the following:

- Locate all new MCPS computer or communications centers in an area unlikely to experience natural disasters, serious or man-made accidents, and related problems.
- Construct new and remodeled MCPS client server facilities to protect against fire, water damage, vandalism, and other threats that may occur.
- Select the location of multi-computer or communications facilities to minimize the risk of damage:
 - Locate facilities above the ground floor to minimize the chances of water damage and theft.
 - Locate kitchen facilities away from, but not directly above or below, computer facilities.
 - Do not locate restroom facilities directly above computer facilities to minimize the risk of water damage.
 - Do not locate computer facilities adjacent to an exterior wall to protect the systems from unauthorized electromagnetic eavesdropping and damage from bombs.
- Whenever possible, design MCPS communications networks so that there is not one single point of failure, such as a central switching center, that could affect the availability of network services.
- Back up all critical information and software on a regular schedule (see section 3.0, Electronic Data Security). The CTO or designee will assign a person to perform school and office backups. Use of redundant system protections for mission critical systems and applications is required.
- Store systemwide critical information and software in a physically separate, environmentally controlled facility. This facility is to be at least five miles from the site where original copies reside. Additionally, house all current supporting materials needed for disaster recovery, such as manuals, charts, and diagrams, together at the same facility. Supporting materials include anything required by MCPS departments or units that are necessary to maintain day-to-day mission-critical operations until recovery. Store backups for other sites in a secure, environmentally controlled container and room. Periodically test the backups for viability.
- List all archival backup data that is stored off-site in a current directory that shows the date when the information was last modified, and the content of the information. All media that is used to store sensitive, valuable, or critical information for longer than six months must not be subject to rapid degradation. Copy this information to newer media before the time limits suggested by the manufacturer are exceeded.

OCTO must prepare, periodically update, and regularly test information technology emergency response plans for computer and communications systems. The disaster recovery plan

- provides for the continued operation of critical systems in the event of an interruption or degradation of service;
- allows all critical computer and communication systems to be available in the event of a major loss, such as, a flood, earthquake, or tornado; and
- prioritizes the sequence of critical systems being recovered.

5.0 Systems and Applications Security

Before MCPS enterprise applications and systems are developed, acquired, or modified, management of the involved user department must work with IARM to clearly specify and document the relevant security requirements. For all application systems, system designers and developers must consider security from the beginning of the system design process through conversion to a production system. Typically the systems development life cycle will involve several points where security is formally included in the process. Technical staff is required to consider security as a formal part of the systems development life cycle. This includes systems developed in partnership with third party vendors. All systems or applications developed with outside vendors require written agreements protecting MCPS data and IT resources.

5.1 Application Code Vulnerabilities

IT staff is to exercise “due care” by verifying that systems and applications, whether MCPS-developed or vendor-supplied, are secure using MCPS-approved, industry-standard tools. Working with IARM, system developers identify the critical elements to apply for readiness assessment prior to deployment.¹ Each of the following five categories should be considered and assessed at the appropriate point in the systems development life cycle:

- Security-related functions
- Input/output validation and encoding errors
- Error handling and logging vulnerabilities
- Insecure components
- Coding errors

¹ Berg, Ryan, *The Path to a Secure Application, A Source Code Security Review Checklist*, OUNCE Labs, Waltham, MA, 2007.

Category	Vulnerability	Risk
Security-related functions	Weak or nonstandard cryptography	Attackers can break algorithms to steal sensitive data
	Non-secure network communications	Legitimate methods of sending information are not documented or protected, exposing critical data
	Application configuration vulnerabilities	Access to unprotected configuration files or options allows manipulation of software properties or data
	Access control vulnerabilities	Unauthorized access to confidential data and resources
	Unprotected database and file system use	Hijacking and manipulating calls to databases and file systems expose data
	Dynamic code vulnerabilities	Successfully inserting malicious commands into applications that load dynamic code without proper validation
	Native code loading	Manipulating these system-level calls allows for data manipulation, exposure, or destruction
	Data storage vulnerability	Data stored insecurely can easily be stolen
	Authentication errors	Attackers use legitimate users' credentials to steal or manipulate data
Input/Output validation and encoding errors	SQL injection vulnerabilities	Sending SQL commands directly to databases to steal or manipulate data
	Cross-site scripting vulnerabilities	Users unknowingly have sessions hijacked, download Trojans, or fall for phishing scams
	OS injection vulnerabilities	Attackers modify or misuse operating system commands to control data and resources
	Custom cookie/hidden field manipulation	Creates a level of trust attackers can manipulate to execute attacks such as SQL injection or cross-site scripting
Error handling and logging vulnerabilities	Insecure error handling	Furnishes attackers with information they can use for attacks
	Insecure or inadequate logging	Accessible log files divulge information useful for attacks, while inadequate logging allows attacker to hide tracks
Insecure components	Malicious Code	Seemingly legitimate code inserted into software can allow attackers to circumvent security measures
	Unsafe native methods	Unchecked use of native methods provides entrée for attackers to access critical resources such as system or environment memory
	Unsupported methods	Undocumented functions or routines can be a hidden source of insecurity for potential exploitation

Coding errors	Buffer overflow vulnerabilities	Attackers can hijack system resources.
	Format string vulnerabilities	Leads to buffer overflows or data exposure
	Denial of service errors	Prevents software from functioning
	Privilege escalation vulnerabilities	Attackers can access confidential data and resources
	Race conditions	Circumventing an application process to manipulate operations
	Unsafe native method use	May sacrifice security for performance, allowing unsafe access to system or environment memory
	Unsupported method	Legitimate operations may unknowingly invoke calls to vulnerable code

5.2 Security of Web-based Applications

Security of web-based applications development should include the following phases² based upon the specific requirements of the application:

- ✓ Examination of external/client-side visible code for information that may open the application to attack.
- ✓ Inspection of application validation and bounds checking for both accidental and mischievous input.
- ✓ Manipulation of client-side code and locally stored information.
- ✓ Examination of application-to-application interaction between system components such as the web service and back-end data sources.
- ✓ Discovery of techniques that could be employed by attackers to escalate their permissions by referencing application components with higher server-side permissions.
- ✓ Attempts to subvert in-transit data between the client and server system. Examination of data delivery methods and the likelihood of their subversion or use in a replay-type attack, or other session orientated attacks, including an analysis of system responses to such data.
- ✓ Authentication methods in use are examined for their robustness and resilience to various subversion techniques. Attempts are made to bypass authentication processes and/or impersonate valid logged-in users. Detailed studies of user segregation methods are undertaken and an analysis of server-side responses to failed attempts is made.
- ✓ Overall examination of the application's deployment and security configuration from perceived threat models. Advice is given on secure deployment methodologies for the application type, based upon market considerations, new vulnerability developments and attack methodologies.

² Ollmann, Gunter, *Application Security Assessments, Advice on Assessing your Custom Application*, www.technicalinfo.net.

6.0 Telecommunications Security

6.1 Wide Area Network/Local Area Network (WAN/LAN)

Computer system security is never to be totally dependent on the security of another computer system. Access to offices, computer rooms, and work areas that contain sensitive information must be physically restricted. Managers who are responsible for employees working in these locations must determine the appropriate access controls. Employees must not attempt to enter restricted MCPS areas without authorization to do so.

Every MCPS multi-user computer system, including local area network servers and private branch exchange switches must have a designated security administrator. The security administrator is responsible for defining user privileges and monitoring access control logs. The designated security administrator should inform the appropriate department/division in OCTO of the name and contact information for this individual.

The security administrator for each multi-user computer system must designate and train an employee to act as their backup as necessary. Inform the appropriate department/division in OCTO of the name and contact information for this individual. If this is a temporary assignment, staff may inform the Help Desk instead.

Users are not to disable or modify security measures installed on any computer for any reason without permission from the appropriate staff: ITSS, local security administrator, or technology system maintenance staff. Security measures include such things as menuing software, operating systems settings, and anti-virus software. If security measures are disabled to perform a hardware or software installation, they must be reactivated when the installation is completed.

OCTO must organize and maintain in-house computer emergency response teams. These response teams will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies, such as virus infestations, hackers, and break-ins.

All critical members of OCTO computer emergency response teams must have a backup person or provide contact information if available. OCTO emergency procedures should document and maintain the names and phone numbers of response team members.

Connections between MCPS internal networks and the Internet or other accessible networks must have an approved firewall and related access controls.

6.2 Internet Use

Levels of access to the Internet will be provided to those users with a legitimate need for this access. The following levels of access may be granted with approval of the appropriate authorities (parent, teacher, or administrator):

- Access to use the Internet
- Access to post files on Internet servers for a specific directory
- Access to manage security on Internet server

Internet use should support education and research and be consistent with the MCPS mission. Use of the Internet will be in accordance with the school system's regulations on acceptable use and students' rights and responsibilities. For example, staff use of the Internet may be for the following:

- Administrative systems
- Student information
- Professional development, research, and communication
- Human resources and financial systems
- Information for educational research, curriculum, and school activities
- Other appropriate information in the support of the MCPS mission

The Internet may not be used for the following:

- Viewing information that is sexually explicit, racist, violent, or otherwise potentially offensive and does not serve an educational purpose
- Accessing or disseminating unauthorized information
- Distorting or misrepresenting information
- Introducing viruses
- Sharing passwords, accounts, and e-mail addresses
- Copying or transferring copyrighted materials without authorization or any other violation of copyright law
- Illegal activities
- Disseminating sensitive information to unauthorized users
- Sending unsecured information that may be confidential or private

Users are not to establish Internet or other external network connections that permit non-MCPS users access to MCPS systems and information without prior approval from the CTO. Requests for exceptions should be sent in writing from the principal or supervisor.

Internet access from MCPS networked computers must be provided by the MCPS Internet connection. Schools and offices are prohibited from establishing alternative Internet connections. Special exception requests should be directed to the director, Department of Infrastructure and Operations, OCTO.

MCPS web pages are not to disclose personal information about students. Student's home addresses and phone numbers must not be posted on web pages. The names of students are not to be posted if the parent has withheld consent on the fall directory information form. Parental permission also is needed to post the following:

- Student e-mail addresses
- Photographs identifying individual students by their full name
- Graphics or text that identify a student as being in special education

Web pages and embedded hyperlinks are not to post banned information. Examples of banned information includes information that

- Jeopardizes MCPS data security
- Violates the privacy of others
- Jeopardizes the safety and health of students and employees
- Contains obscene or libelous material
- Causes disruption of school or business activities
- Encourages activities such as riots or destroying property
- Violates copyright laws
- Plagiarizes the work of others
- Advertises a commercial business
- Appears on the Web site without the approval of the administrator or their designee

The principal or supervisor at the site is responsible for web page content posted by that location. MCPS employees are to notify their administrator or their designee if they know a web page contains questionable material. The administrator is to determine if any applicable policies, guidelines, rules, or regulations have been violated before taking action.

6.2.1 Electronic Mail (E-mail)

Every MCPS employee who uses computers in the course of their regular job duties will be granted an Internet e-mail address and related privileges. All MCPS communications sent by electronic mail must be sent and received using this company e-mail address. A personal Internet service provider e-mail account or any other e-mail address must not be used for MCPS business unless a worker obtains management approval. When transmitting messages to groups of people outside MCPS, workers must always use either the blind carbon copy facility or the distribution list facility. Unsolicited e-mail transmissions to prospects and customers are prohibited. Emotional outbursts sent through e-mail and overloading the e-mail account of someone through a deluge of messages are forbidden. All business e-mail communications must be proofread before they are sent and be professional and businesslike in both tone and appearance. All MCPS employees must refrain from sending credit card numbers, passwords, or other sensitive information that might be intercepted.

MCPS uses Microsoft Outlook and Microsoft Outlook Web Access (OWA) for e-mail communications. Microsoft Outlook requires a direct connection to the MCPS enterprise network while OWA provides remote access over a public Internet connection.

MCPS incorporates Exchange messaging protocol (also known as MIME) for sending and receiving electronic mail messages. To improve messaging security, other messaging protocols

such as POP and IMAP currently are not provided. Remote Procedure Call (RPC) over Hypertext Transfer Protocol (HTTP) is used to allow remote Outlook clients to securely and remotely communicate with the MCPS Exchange server.

6.2.2 Electronic Mail (E-mail) Retention

MCPS has established the e-mail retention policy to be set at 30 days. This means 30 days after creation of an e-mail, that message will be automatically deleted from MCPS Outlook accounts and the servers. Any e-mails needing to be retained longer than 30 days must be stored separately. All electronic communications are discoverable and must be provided when issued a subpoena by the legal system.

6.3 Remote Access

MCPS supports only Transmission Control Protocol/Internet Protocol (TCP/IP) for remote access. Remote access information is not to be disclosed.

Internal address configurations and related MCPS system design information for network computer systems must be restricted. Information about access to MCPS computer and communications systems, such as Internet protocol addresses, server names, and dial-up modem telephone numbers is confidential. Restrictions are necessary to ensure that both systems and users outside the internal network are unable to access this information without approval from the OCTO.

One primary means of remote access for employees and vendors is through virtual private networking (VPN). Users of the VPN server are expected to abide by the same guidelines as that of the MCPS private network. With VPN users are connected directly to the MCPS network and are restricted to the same access as when connected to the network directly. Access to any other systems or devices without authorization is prohibited. Also, access to the network using VPN software is meant for the assigned user. Providing VPN access to any unauthorized users or devices is strictly prohibited.

Third-party vendors must have a legitimate business need before they are given remote-access privileges. These privileges are temporary and granted only for the time required to complete their work. The vendor must sign a remote access agreement and receive approval from the CTO.

MCPS also uses wireless technology for extending network access, including, but not limited to laptops, net books, cell phones and Personal Digital Assistants (PDAs). The wireless access points that provide this service meet specific technical requirements as determined by the MCPS technology standards. Wireless access points, wireless devices, or any other mobile technology not supplied or pre-approved by MCPS are not permitted. Any devices that are permitted to access the wireless network must be password protected. This includes smart phone devices for remote e-mail access.

6.3.1 Security Considerations

The following are security considerations for remote access:

- MCPS computers that can be reached by third-party networks such as dial-up lines, value-added networks, and the Internet, must be protected by an access control system that defines how privileges are granted. Access system design and implementation must be approved by the CTO.
 - Remote access connections (such as dial-up and VPN) to the MCPS computer data network require extended user authentication to positively identify the user. These systems include call-back, tokens or smart cards, and other approved technologies that provide more security than fixed password systems.
 - Direct connections between MCPS systems and computers at external organizations via the Internet or any other public network are prohibited unless they pass through additional access control points, such as a firewall, and have been approved by the CTO.
 - In order to access the MCPS computer network, every third party must secure its own connected system by methods consistent with MCPS requirements. MCPS reserves the right to audit security measures on connected systems without prior warning and to terminate network connections to third party systems that do not meet MCPS requirements.

6.3.2 Teleworking

Teleworking is not a universal employee benefit and is covered by MCPS Regulation GEH-RA, *Teleworking*. The employee's administrator must validate that working at an alternative work site is appropriate for the work assigned. The administrator must ensure that physical and information security meets MCPS security requirements. Permission must be requested through the appropriate deputy superintendent the Office of Human Resources. If access is granted, the user must sign a remote access agreement and submit to the CTO for implementation.

The following specific security requirements are applicable to teleworking:

- Teleworkers must ensure compliance with MCPS remote access security procedures. As a condition of continued employment, teleworkers must abide by all remote access security procedures, such as, compliance with software license agreements, use of current anti-virus software, performance of regular backups, and securing of data. Users must log off when the session is complete.
- MCPS reserves the right to inspect teleworkers' sites with one or more days advance notice.
- The CTO must approve all remote access to the MCPS network. When computers and other networking devices are connected to the MCPS network via remote access, it is expected that no other connections to the Internet or other foreign networks are made. Remote access is meant to be exclusive to the authorized device and the MCPS network. Remote access and control software, such as PC Anywhere, is not to be installed without written authorization.

6.4 Protecting MCPS Assigned Computing Equipment

MCPS provides appropriate mobile technology equipment for staff members in accordance with their work requirements. The assigned equipment is intended for use for educational purposes only and is not intended as a replacement for any equipment that may be owned personally. Use of the MCPS equipment for personal purposes should be within the standards of good judgment and common sense and in compliance with the IGT-RA.

The staff member has the responsibility to take appropriate precautions to prevent damage to or loss/theft of an MCPS-assigned laptop computer. If the laptop is lost or stolen, it must be reported to OCTO immediately. Theft or loss away from MCPS facilities should also be reported to local police. The police report should include the serial number of the lost computer. A copy of the police report must be sent to OCTO within 24 hours of the discovery of the loss.

6.5 Surveillance Cameras (CCTV)

MCPS uses surveillance cameras in locations throughout MCPS. The cameras and the servers connected are restricted to authorized users. Any use of the software or access to the camera feeds must be approved by the Department of School Safety and Security.

7.0 Investigations

In the event of a violation of IGT-RA, *User Responsibilities for Computer Systems, Electronic Information, and Network Security*, an investigation will be conducted upon the reporting of the event to the IARM supervisor.

All requests for investigations must be forwarded to the CTO. Once the request for investigation is approved, the IARM supervisor will facilitate the investigation process. The process will include, but is not limited to, interviews with staff or students, forensics investigations, and/or involve reporting to the police or police forensics investigations. The IARM supervisor will report all findings to the CTO and all other appropriate administrative staff.

8.0 E-Discovery

Electronic discovery refers to any process in which electronic data are sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

8.1 Notice of claim

Notice of claim is received from the Office of the County Attorney for specific claims against MCPS or staff. The staff is notified of the claim and instructed to preserve and protect all electronic messages and documents related to the claim until otherwise instructed. All parties involved will receive an email providing them with instructions and points of contact. Specific email stores are copied and stored on a secure server for e-discovery. All other paper and electronic documents must be protected by the individual's identified on the claim.

9.0 Noncompliance

MCPS access assures compliance with Internet policies and will assist with internal investigations. All electronic mail messages, files on personal computers, web browser cache

files, files on servers, Web browser bookmarks, and other information stored on or transmitted by MCPS computers are subject to be reviewed, copied, stored, archived, and monitored for violation of MCPS regulations and local, state, or federal laws.

All MCPS staff and authorized network users are responsible for protecting the integrity of MCPS data by taking responsible steps to prevent those without the appropriate access levels from obtaining the data. Anyone aware or suspicious of inappropriate data use or possible security breaches should alert their immediate supervisor. The supervisor should follow up by contacting OCTO.

The following tables summarize possible infractions and penalty options for employees, retirees, volunteers, and students.

Employees, Retirees, and Volunteers

Infraction	Minimum Penalty	Maximum Penalty
<p>Computer Abuse, see IGT-RA; examples include but are not limited to the following:</p> <ul style="list-style-type: none"> • Hacking into MCPS/CESC network • Hacking into school network • Intentional viewing of inappropriate/sexually explicit material • Intentional distribution of inappropriate/sexually explicit material • Intentional viewing of child pornography • Intentional distribution of child pornography • Misuse of the network privileges • Misuse of e-mail privileges • Written electronic abuse/harassment • Written electronic threats 	Written Reprimand	Termination Restitution Police referral

Students

Infraction	Minimum Penalty	Maximum Penalty
<p>Computer Abuse; examples include but are not limited to the following:</p> <ul style="list-style-type: none"> • Hacking into MCPS/CESC network • Hacking into school network • Intentional viewing of inappropriate/sexually explicit material • Intentional distribution of inappropriate/sexually explicit material • Intentional viewing of child pornography • Intentional distribution of child pornography • Misuse of the network privileges • Misuse of e-mail privileges 	<p>Loss of Computer Privileges Restitution</p>	<p>Recommendation for Expulsion Restitution Police Referral</p>
<p>Bullying, see JFA-RA</p> <ul style="list-style-type: none"> • Written electronic abuse/harassment • Written electronic threats • Sexual Harassment 	<p>Conference</p>	<p>Recommendation for Expulsion</p>

Appendix: Abbreviations

CESC	Carver Educational Services Center
CTO	Chief Technology Officer
IARM	Information Assurance and Risk Management
ID	Identification
IT	Information Technology
ITSS	Information Technology Systems Specialist
MCPS	Montgomery County Public Schools
MELT	MCPS Employee Login Table
NSBO	Nonschool-based Office
OCTO	Office of the Chief Technology Officer
OS	Operating System
OSX	Operating System Extension
OWA	Outlook Web Access
PTA	Parent Teacher Association
VPN	Virtual Private Network