

BOARD OF EDUCATION OF HOWARD COUNTY
MEETING AGENDA ITEM

TITLE: Policy 3040 Technology Security (New) **DATE:** January 14, 2010
PRESENTERS: Michael Borkoski, Technology Officer
Nick Vissari, Technology Security Analyst

OVERVIEW:

Policy 3040 was developed under the guidelines for policy development and adoption. The Committee Charter was approved by the Superintendent on August 24, 2009. A committee of stakeholders, chaired by Michael Borkoski and Nick Vissari, was convened to make recommendations for the development of the policy. The committee was charged with the following tasks:

- Establish a clear and consistent framework for security applicability within all facets of Howard County Public School System (HCPSS) technology including the recommendations provided by the State of Maryland Office of Legislative Audits and the Clifton Gunderson LLP annual financial audit
- Develop policy with up-to-date legal references and ensure compliance with legal and regulatory mandates, including the Health Insurance Portability and Accountability Act (HIPAA), the Family Education Rights and Privacy Act (FERPA), and the Child Internet Protection Act (CIPA)
- Recommend language that assures awareness and communicates expectations regarding potential information technology security risks to the HCPSS data in critical areas of need
- Review the policy for consistency with other school system policies, with particular attention for consistency with the revised Policy 8080 Acceptable Use of Computer Technology
- Make recommendations as appropriate in accordance with current best practices and system requirements
- Recommend language as needed to address policy standards outlined in Policy 2020 Policy Development and Adoption
- Note any implications or follow-up work that may be necessary as a result of the committee's recommendations.

Attached are highlights of the committee's work, a list of committee members, and the proposed policy and implementation procedures. The committee's recommendation was submitted to the Superintendent's Cabinet on November 9, 2009. A report was presented to the Board on December 10, 2009.

RECOMMENDATION/FUTURE DIRECTION:

Take action to adopt new Policy 3040 on February 11, 2010. The new policy would become effective July 1, 2010.

**Submitted
by:**

Michael Borkoski
Technology Officer

Nick Vissari
Technology Security Analyst

**Approval/
Concurrence:**

Sandra Erickson
Deputy Superintendent

Mamie Perkins
Chief of Staff

Theresa Alban
Chief Operating Officer

**Policy 3040 Technology Security (new)
Highlights of Initial Proposal**

Policy

- States the Board of Education commitment to providing a clear and consistent technology security plan throughout the HCPSS
- States that the HCPSS will ensure compliance with all local and regulatory mandates
- Establishes standards that clearly delineate technology requirements
- Establishes that all staff will comply with the expectations for a secure technology environment
- Sets a standard for access control
- Clarifies physical security for all data centers, main distribution frames, and intermediate distribution frames
- Adds compliance statements for the Superintendent, school principals, the Technology Security Analyst, and supervisors
- Adds references, legal and local.

Implementation Procedures

- Specifies guidelines for annual announcements and dissemination of information regarding technology security procedures
- Clarifies regulations regarding electronic communications
- Includes guidelines for online testing
- Clarifies security vulnerability assessments
- Separates employee user guidelines from student user guidelines
- Discusses reporting procedures in the case of a suspected violation of this policy.

**Committee for the Development of
New Policy 3040 Technology Security**

Michael Borkoski, Technology Officer*

Nick Vissari, Technology Security Analyst*

John Cheek, Mt. Hebron HS, Assistant Principal

Mark Coates, Secondary Curricular Programs

Ted Mallo, Community Advisory Council (CAC)

Kedre' Fairley, Assistant Principal, Howard HS

Tim Guy, Howard County Education Association (HCEA)

Arlene Harrison, Elementary Administrative Director

Carolyn Jameson, Howard County Administrators Association (HCAA)

Ted Ludicke, Technology Specialist

Ken Mason, Software Developer

Debbie O'Byrne, Assistant Principal, Mt. View MS (HCAA)

Katherine Orlando, Principal, Worthington ES

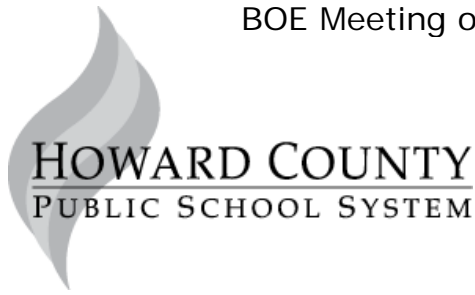
Davina Pruitt-Mentle, Technology Advisory Committee (TAC)

Alvin Thompson, Equity Council

Rich Weisenhoff, Career & Technology Education (CTE) Coordinator

Julie Wray, Media and Technology Education

**Committee Chairperson*



I. Policy Statement

The Board of Education recognizes the value of technology security throughout the Howard County Public School System (HCPSS). The Board values the need for a clear and consistent technology security plan that promotes awareness and communicates expectations for safeguarding and securing HCPSS information and technology. The Board also recognizes that all HCPSS technology users must remain in compliance with legal and regulatory mandates.

II. Purpose

The purpose of this policy is to provide guidelines for maintaining the confidentiality, integrity, safety, and availability of HCPSS data and resources. This policy will provide guidance in the areas of access controls, asset management, network security, physical security, remote access, and technology security incident response.

III. Definitions

Within the context of this policy, the following definitions apply:

- A. Account Credentials – Any data or object used specifically for the purpose of gaining access (authenticating) to an electronic system, usually a username and password combination.
- B. Banner Text – The notification sent to an end user prior to authentication on a system.
- C. Computer System – Any electronic medium that can execute a set of instructions designed to perform a specified task.
- D. Data Center – A dedicated area of a building that supplies the electrical necessities and environmental conditions required to operate servers, network technology, and other electronic systems.
- E. Intermediate Distribution Frame (IDF) – A non-primary distribution area for data cables from the main distribution frame.
- F. Least Possible Privilege – The methodology whereby each user is assigned only the appropriate level of access needed for their responsibilities.

-
- G. Main Distribution Frame (MDF) – The primary distribution area for connecting HCPSS equipment to subscriber carrier equipment.
 - H. Network – The physical means of transmitting data between systems; includes wired and wireless technologies.
 - I. Online Resource – Any electronic system which can be accessed remotely for the purpose of viewing or manipulating data which can exist on the Internet or on a local area network.
 - J. Production System – The technology used to electronically implement HCPSS operations.
 - K. Software – Any application that can be executed on a computer system, server, or other electronic device.
 - L. Systems Administrator – The person responsible for implementing, managing, and maintaining HCPSS technology.
 - M. Technology – Electronic systems including, but not limited to, computer systems, servers, telephones, facsimile equipment, cellular phones, portable electronic devices, network infrastructure, online resources, e-mail, and all data stored or transmitted electronically.
 - N. Technology Security Analyst – The person responsible for ensuring that all HCPSS technology is implemented securely in compliance with legal and regulatory mandates regarding electronic systems.

IV. Standards

- A. Protection of HCPSS technology systems
 - 1. HCPSS reserves the right to take all necessary actions to prevent its network and computing infrastructure from being used to attack, damage, harm, or improperly exploit any internal or external systems or networks. Use of the HCPSS network to gain or attempt to gain unauthorized access to any system or information is prohibited.
 - 2. Software and network protocols not essential to carrying out the mission of the HCPSS or to the conduct of HCPSS business should be used with caution. Should such software or network protocol become a risk to the security of the HCPSS technology systems, its use will be restricted or blocked as deemed appropriate or necessary by the Systems Administrator/Designee, without prior notice.

3. HCPSS reserves the right to take all necessary actions to protect the integrity of its network, the systems attached to it, and the data contained therein.

B. Access Controls

1. Access to HCPSS technology will be provided in accordance with the procedures of this policy.
2. The HCPSS has the right to archive, audit, or purge the contents of electronic communications, files, and other material created, stored, or accessed using HCPSS technology.
3. The HCPSS has the right to access or disclose, for investigative purposes, the contents of electronic communications, files, and other material created, stored, or accessed using HCPSS technology. Access or disclosure can only be authorized by the Superintendent or General Counsel.
4. The HCPSS will maintain a process for creating, managing, and documenting account credentials.
5. Access to HCPSS technology, granted by virtue of the user's status as an employee or student, will be terminated when the relationship is terminated or the purpose is fulfilled.
6. The Systems Administrator's designee will review system and network audit logs at least one time per day. Suspicious items will be logged and reported to the Technology Security Analyst/Designee for further investigation in accordance to this policy.
7. HCPSS users will be required to authenticate to HCPSS computers and servers using individual account credentials.
8. HCPSS users are prohibited from sharing individual account credentials.
9. HCPSS users are granted access to data and resources based on a "least possible privileges" methodology.

C. Asset Management

1. All technology assets will be accounted for and tracked by location, by cost, and by functionality in an automated system.
2. All technology assets must be disposed of in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88.

D. Network Security

1. All HCPSS technology networks will be configured to protect from unauthorized access at all entry points.
2. Users are prohibited from connecting non-HCPSS owned technology to any HCPSS network without prior written approval from the Systems Administrator/Designee.
3. The HCPSS will provide remote network and system access on an as-needed basis.
4. The HCPSS will employ technologies, where appropriate, to ensure compliance with all local and regulatory mandates and other policies.
5. Users must not use wireless technologies in a manner that could compromise the security of HCPSS technology.
6. The HCPSS prohibits the use of remote network access software and utilities without prior written approval from the Technology Security Analyst/Designee.
7. The HCPSS may employ banner text to provide notice of legal rights and responsibilities to users of HCPSS computer networks and online resources.
8. The HCPSS will establish security incident response guidelines for all production systems.

E. Physical Security

1. Physical access to technology resources, data centers, main distribution frames (MDFs) and intermediate distribution frames (IDFs) will be controlled to prevent and detect unauthorized access to these areas. Access to these resources and areas will be granted to those persons who have legitimate business responsibilities in those areas.
2. All data centers will be secured using technologies that monitor individual access and provide auditable access logs.

F. Other Provisions

1. Notice of the provisions of this policy and user responsibilities will be communicated to all students, parents, employees, and users of HCPSS technology.

2. Failure by any user to comply with this policy will result in the temporary or permanent termination of technology access privileges, in addition to any applicable disciplinary action or financial obligation.

V. Compliance

- A. The Superintendent/Designee will establish guidelines and appropriate forms for the acceptable use of technology.
- B. The Superintendent/Designee is responsible for communicating and educating all users in the provisions of this policy annually through customary channels.
- C. The Superintendent/Designee is responsible for reviewing this policy at least every three years and recommending it for revision as necessary.
- D. Principals and supervisors are responsible for notifying and educating students, families, and employees in their schools and offices of the provisions of this policy.
- E. Principals and supervisors are responsible for notifying and educating students, families, and employees in their schools and offices of all end-of-year and end-of-employment check-out procedures.
- F. The Technology Security Analyst is responsible for establishing prudent measures to safeguard the security of HCPSS technology in accordance with Policy 8080 Acceptable Use of Technology.
- G. The Office of Community Services is responsible for notifying individuals or organizations seeking to use school system technology as part of an agreement to use school system facilities (Policy 10020 Use of School Facilities by Non-School Groups) of the provisions of this policy.

VI. Delegation of Authority

The Superintendent is authorized to develop procedures for the implementation of this policy.

VII. References

- A. Legal
Electronic Communications Privacy Act, 18 U.S.C. §2701-2711
Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g)
Section 508 of the Rehabilitation Act of 1973, 20 U.S.C. §794(d)

Title VII of the Civil Rights Act of 1964, 42 U.S.C. §2000(e)
Title XVII, Children’s Internet Protection Act, as codified at 47 U.S.C. §254(h)

B. Other Board Policies

- Policy 4040 Fixed Assets
- Policy 7030 Employee Discipline
- Policy 8080 Acceptable Use of Technology
- Policy 8120 Testing: State and Local Responsibilities and Protocols
- Policy 9030 Student Publications and Productions
- Policy 9050 Student Records and Confidentiality
- Policy 9200 Discipline
- Policy 10010 Distribution and Display of Materials and Announcements
- Policy 10020 Use of School Facilities by Non-School Groups

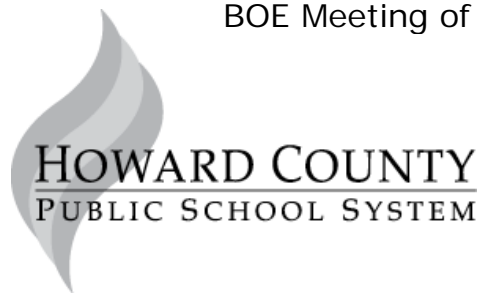
C. Other

- Ethics Regulations
- National Institute of Standards and Technology (NIST) Special Publication
800-88
- Student Code of Conduct
- Technology Security Incident Handling Form
- User Guidelines (Staff Email Guidelines, etc.)

ADOPTED: February 11, 2010

AMENDED:

EFFECTIVE: **July 1, 2010**



POLICY 3040-PR
IMPLEMENTATION PROCEDURES
TECHNOLOGY SECURITY

Effective: July 1, 2010

I. Dissemination of Information

- A. Notification of the provisions of this policy and these implementation procedures will be given annually to all students, families, employees, and service providers. Methods may include:
1. Announcements in schools over the public address system at the beginning of the school year and at other times as appropriate
 2. Publications in school and system newsletters, handbooks, and other documents
 3. Notifications posted in areas that provide access to technology (e.g., media center, computer lab)
 4. Notifications posted on school and system websites
 5. Reviews for students by classroom teachers, media specialists, or other appropriate employees
 6. Incorporated, whenever possible and appropriate, into the process of accessing software and/or files.
- B. Principals are responsible for notifying all students, families, employees, volunteers, contractors, and interns in their schools of the responsibilities of users of Howard County Public School System (HCPSS) technology and of guidelines for network activities at the beginning of the school year, with reminders as necessary.
- C. Department supervisors are responsible for notifying those under their supervision of the provisions of this policy and these implementation procedures annually.
- D. The Office of Community Services is responsible for notifying individuals or organizations approved to use HCPSS technology as part of an agreement to use HCPSS facilities (Policy 10020 Use of School Facilities by Non-School Groups) of the provisions of this policy and these implementation procedures.

II. General Procedures

- A. Electronic Communications

1. All electronic communications created, received, or stored on HCPSS electronic communications systems are the sole property of the HCPSS and not the author, recipient, or user.
2. Users will have no expectation as to the privacy or confidentiality of any electronic communication using HCPSS electronic communications systems.
3. Users must not use HCPSS electronic communications systems for commercial, profitable, religious, or political use.
4. Users must not use HCPSS electronic communications systems to transmit messages, images, cartoons, epithets, or slurs based upon age, race, national origin, marital status, sexual orientation, gender, gender identity, disability, ethnicity, or religious affiliation as defined in Policy 1000 Civility.
5. HCPSS systems that store or transmit employee data, student record data, financial data, or other legally confidential data will implement appropriate authentication technologies to prevent unauthorized access or modification.
6. Users of HCPSS electronic communications systems must ensure that both their usage and electronic communications content are in compliance with all other HCPSS policies.

B. Online Testing

1. All online testing will be conducted in accordance with the guidelines, policies, and procedures set forth by the governing agency.
2. All data saved to computers and servers for the purposes of online testing administration and execution will be deleted in accordance with the guidelines, policies, and procedures set forth by the governing agency.

C. Security Vulnerability Assessments

1. The Technology Security Analyst/Designee will coordinate the performance of annual network and system security vulnerability assessments to ensure compliance with local and legal regulatory mandates. These assessments will focus on all networking, student data, personnel, financial, and communications systems.
2. The HCPSS may contract with third party companies or individuals to perform external security vulnerability assessments and penetration tests.

D. Technology Security Incident Response

1. All HCPSS technology security investigations will be authorized by the Chief Operating Officer.
2. The Technology Security Analyst/Designee reserves the right to access, intercept, and/or record all non-identifiable HCPSS electronic communications, files, and other data for investigative purposes.
3. The Technology Security Analyst/Designee reserves the right to access, intercept, and/or record identifiable content of HCPSS electronic communications, files, and other data with prior approval from the Superintendent or General Counsel.
4. The Technology Security Analyst/Designee will document all HCPSS technology security investigations using the HCPSS Technology Security Incident Handling Form.
5. The Technology Security Analyst/Designee will conduct all HCPSS technology security incident investigations in strict confidence. All information pertaining to HCPSS technology security investigations will be forwarded to the Chief Operating Officer for appropriate handling, dissemination, and disposal.

E. Storage Media Handling and Disposal

1. Access to HCPSS storage media including, but not limited to, floppy disks, hard disks, CDs, DVDs, firewire drives, USB memory sticks, etc., must be secured utilizing the “least possible privileges” methodology.
2. All service to HCPSS computers and servers must be performed onsite by authorized HCPSS personnel or authorized contractors. If a computer or server must be taken offsite for service, all hard drives, CDs, and DVDs must be removed prior to the equipment leaving the premises. If removal of any/all hard disks, CDs, or DVDs is not feasible, prior approval must be obtained in writing by the Systems Administrator/Designee to remove the equipment.
3. All HCPSS storage media including, but not limited to, floppy disks, hard disks, CDs, DVDs, firewire drives, USB memory sticks, etc., must be disposed of in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88.

F. Systems Development Life Cycle

1. All HCPSS applications and systems must be developed or procured in compliance with all local and legal regulatory mandates.
2. When feasible, all HCPSS applications and systems will employ the latest software versions and patch levels to ensure maximum functionality and security.
3. All HCPSS application and system test data must be fictional.
4. The HCPSS must not use production data in test systems or use test data in production systems without prior approval, in writing, from the Systems Administrator/Designee.
5. All HCPSS application and system source code will be managed in a controlled auditable environment.
6. All HCPSS production systems will have an established product life cycle that defines requirements to ensure sustainability of the systems over time.

G. System Security Guidelines

1. HCPSS reserves the right to employ technology security measures.
2. Users must not attempt to circumvent, modify, or disable technology security measures implemented by the HCPSS. These include but are not limited to:
 - a. Anti-malware software
 - b. Internet content filter
 - c. Microsoft Active Directory Group Policy
 - d. Apple Open Directory
 - e. Network firewalls
 - f. Computer and server administrative management software.
3. Wireless access points will be configured utilizing Wi-Fi Protected Access (WPA) or better encryption. The wireless broadcast range will be configured so that it does not exceed the physical perimeter of the building. All exceptions must be approved, in writing, by the Technology Security Analyst/Designee.

H. User Credential Assignment & Use

1. User Credential Assignment Guidelines

-
- a. HCPSS employees will be assigned individual account credentials by the Systems Administrator's designee once employment with the HCPSS has been verified.
 - b. Students will be assigned individual account credentials by the Systems Administrator's designee once enrollment in the HCPSS has been verified.
 - c. Contractors, volunteers, interns, and others will be assigned individual account credentials by the Systems Administrator's designee after approval has been granted by the Technology Security Analyst/Designee.
 - d. User password length and complexity requirements will be established for each system by the Systems Administrator/Designee in order to prevent unauthorized access to or modification of confidential or private data.
 - e. Default user passwords will be unique to the individual recipient.
 - f. Users will be required to change temporary passwords upon next login.

2. Employee Account Credential Guidelines

- a. Passwords must not be the same as the user ID.
- b. Passwords must not be shared with others.
- c. Passwords must be a minimum of eight characters consisting of mixed alphabetic and numeric characters.
- d. Passwords must not contain leading or trailing spaces.
- e. Password changes will be required at various intervals, depending on the system.
- f. Password reuse will be prohibited by not allowing the last ten passwords to be reused with a minimum of at least two days each. For applications and systems that cannot functionally meet this requirement, the most stringent password rules will apply.
- g. Application, system, and directory service passwords will expire every 90 days. All exceptions must be approved, in writing, by the Technology Security Analyst/Designee.
- h. Employee accounts associated with a password will be disabled after five unsuccessful logon attempts.
- i. All employee accounts will be disabled after 120 days of inactivity unless prior approval is obtained, in writing, from the Technology Security Analyst/Designee.
- j. The HCPSS reserves the right to modify employee account credentials for individuals upon change in employment status, as directed by the Superintendent.

3. Student Account Credential Guidelines for Secondary Schools

- a. Passwords must not be the same as the user ID.
- b. Passwords must not be shared with others.
- c. Passwords must be a minimum of six characters consisting of mixed alphabetic and numeric characters.
- d. Passwords must not contain leading or trailing spaces.
- e. Password changes will be required at various intervals, depending on the system.
- f. Password reuse will be prohibited by not allowing the last ten passwords to be reused with a minimum of at least two days each. For applications and systems that cannot functionally meet this requirement, the most stringent password rules will apply.
- g. The HCPSS reserves the right to disable student accounts.

III. Violation of Policy

- A. Any person who suspects a violation of this policy or these implementation procedures must report the alleged violation to an appropriate administrator or supervisor for investigation.
- B. The administrator or supervisor must report the suspected violation to the Systems Administrator/Designee.
- C. The Systems Administrator reports the suspected violation to the appropriate chief for follow-through.
- D. In cases of potential harm to an individual, there is a “duty to warn” obligation which requires immediate follow-through and communication with the individual in danger and others who are in a position to protect that individual from harm.

ADOPTED: February 11, 2010

AMENDED:

EFFECTIVE: July 1, 2010