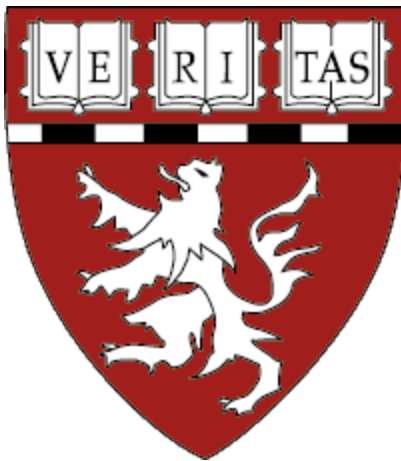


Harvard Medical School Information Security Policy



Contents:

I. Access Control.....	4
II. Fixed Password Management.....	4
III. Third Party Disclosures.....	5
IV. Dissemination of Information.....	5
V. Establishing Network Connections.....	5
VI. Encryption.....	7
VII. Electronic Mail.....	7
VIII. Viruses and Malicious Software.....	8
IX. Personal Use of Information Systems.....	8
X. DMCA (Digital Millennium Copyright Act).....	9
XI. Peer to Peer File Sharing (P2P).....	9
XII. Compromised Systems.....	10
XIII. DMZ.....	10
XIV. Public V. Private IP space.....	11
XV. Firewall Permissions.....	11
XVI. Firewall Requests.....	11
XVII. Internal Firewalls.....	12
XVIII. Wireless Security.....	12
XIX. Networking Device Policy.....	15
XX. HIPAA – Health Insurance Portability and Accountability Act of 1996.....	22
XXI. Technology Resources Utilization.....	22
XXII. Backup Data.....	22
XXIII. Remote Access.....	23
XXIV. Confidential Information.....	23
XXV. Mobile Device Encryption.....	28

Introduction:

Harvard Medical School provides an enterprise class, high speed data network that is used by the students, faculty and staff for the advancement of medical research and education. The data network serves as an indispensable resource toward this goal.

In order to better protect this resource for the use of all, certain measures must be taken to guard against threats both from the outside as well as those that exist inside of the school. It is important to note that the network is a resource to be used by all and, therefore, the misuses and/or abuses of a few individuals will not be tolerated.

This policy document will detail the proper uses and appropriate conduct for users of the high speed data network as well as the HMS Wireless Quad.

I. Access Control

Access Philosophy: Access should be granted to users based on business and/or academic need. Access permissions should not exceed the requirements for a user's job or educational function. I.e. Server and Domain administrators are granted full permissions because of the need to install and maintain the server(s).

Unique User-IDs: Each user is given a unique set of credentials in order to access protected systems. Users should never under any circumstances ever share their user name or password information with anyone. Users will be held responsible for actions performed under their user ID. Shared user accounts, such as "Guest" are not allowed with the exception of certain systems maintained by HMS IT.

Termination of Accounts: Please refer to the HMS Human Resources Policy governing the termination of accounts.

Please consult HMS Human Resources for further information.

II. Fixed Password Management

Choosing Passwords: Users should select passwords of sufficient length and complexity so as to not be easily guessable. These passwords should also not be reflections of the user's personal life. For example, license plate number and spouse's name are both unacceptable passwords. All fixed passwords must be at least eight characters, and where systems support it, this minimum length must be enforced automatically. Users must also choose fixed passwords that include both alphabetic and numeric characters as well as symbols where the systems support it.

Changing Passwords: User-chosen fixed passwords must not be reused or recycled. Switching between two or a similar small number of passwords is therefore prohibited. Where systems support it, fixed passwords must be forced to change every one hundred eighty (180) days. Likewise, where systems support it, expired passwords must be employed. Expired passwords are passwords which must be changed the first time they are used. If Users suspect that somebody else may know their password, the password must be immediately changed. Users forgetting their passwords are provided with a mechanism for resetting via the eCommons web site. Users will be prompted for their "secret question" after selecting Login Problems, Reset Password.

Protecting Passwords: Fixed passwords are a very important way to authenticate the identity of users. Users must not share a fixed password with anyone, including their manager or co-workers. Instead, Users must employ authorized mechanisms to share information such as shared directories, electronic mail, intranet pages, or removable media. Users must not store their fixed passwords in any computer files (such as log-in scripts or computer programs) unless the passwords have been encrypted with encryption software. Likewise, passwords must not be written down unless they have been concealed by a transformation process, or they are physically secured (such as placed in a locked file cabinet). All fixed passwords set by default by the hardware or software vendor must be changed before the involved system can be used for Harvard Medical School activities.

Expectations of Privacy: Users should have no expectation of privacy when using information systems at Harvard Medical School. To manage systems and enforce security, Harvard Medical School may log, review, and otherwise utilize any information stored on or passing through its systems. For these same purposes, Harvard Medical School may also capture user activity such as telephone numbers dialed and web sites visited.

III. Third Party Disclosures

Preauthorization for Public Statements: To maintain customer confidence, all workers who will be delivering speeches, writing papers, or otherwise disclosing information about Harvard Medical School and/or its business must obtain preauthorization from the Public Relations Department. Only designated individuals are authorized to be spokespersons for Harvard Medical School; if a worker is not one of these designated spokespersons, all inquiries from the media must be directed to the Public Relations Department.

Non-Disclosure Agreements: Whenever communications with third parties necessitate the release of sensitive Harvard Medical School information, a standard non-disclosure agreement (NDA) must be signed by the third party. Information released to these third parties must be limited to the topics directly related to the involved project or business relationship.

IV. Dissemination of Information

HMS Information Technology does not disseminate any information pertaining to the architecture and/or security of the network to any parties either by verbal, written, or electronic means.

In certain cases, consultants, vendors and others may be made privy to some level of detail if HMS IT Management deems that the inclusion of such information is necessary.

Likewise no member of Harvard Medical School shall divulge any aspect of the IT Infrastructure without the express consent of a member of HMS IT Management.

V. Establishing Network Connections

Harvard Medical School computers or networks may only be connected to third party computers or networks after the Information Technology Department has determined that the combined systems will be in compliance with Harvard Medical School security requirements. Connections of internal Harvard Medical School computers to the Harvard Medical School internal network (aka intranet) do not require such permissions, unless the involved systems store Confidential or Highly Restricted Information. Likewise, connections to the Internet through Harvard Medical School firewalls do not require such permissions.

Employees of Harvard Medical School must not connect their own computers with Harvard Medical School computers or networks without prior authorization from their department head. Likewise, personally owned systems may not be used to process any Harvard Medical School information unless the systems have first been approved for use by the Information Technology Department.

Employees of Harvard Medical School and vendors working for Harvard Medical School must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, unless they have first obtained written approval from the HMS IT department.

All connections between Harvard Medical School internal networks and the Internet (or any other publicly-accessible computer network) must include an approved firewall or related access control system.

VPN Access: Connections to internal systems that contain sensitive or potentially sensitive data should be encrypted natively within the application that is being used. In the event that this encryption does not exist natively, users should access systems using the approved HMS IT VPN solution. VPN connections should

also be used when accessing sensitive data over a potentially unsecured method such as wireless. VPN accounts may be obtained through the IT Help Desk.

Site to Site VPN access with the HMS Network is not permitted, unless authorized or engineered by HMS IT. There is no reasonable way for HMS IT to verify the integrity of a connecting network, therefore automatic connections to other networks (i.e. Site to Site VPN connections) are prohibited by this policy.

For further information regarding remote access, please refer to section

Third Party Access: Before third party users are permitted to reach HMS internal systems via real-time computer connections (dial-up lines, the Internet, value added networks, etc.), such connections must be approved by HMS IT and may be subject to a security vulnerability assessment.

Third party information system vendors must only be given in-bound connection privileges (Internet, SSH, etc.) when the applicable system manager determines that they have a legitimate business need. These privileges must be enabled only for the time period required to accomplish previously-defined and approved tasks. Third party vendor access which will last longer than one day must be approved by the Information Technology Department.

Unless the relevant information Owner has approved in advance, workers must not place anything other than HMS public information in a directory, on a server, or in any other location where unknown parties could readily access it. One example of this prohibited placement involves posting files to an Internet connected server such that unknown third parties could access these files via FTP services.

As a condition of gaining access to the HMS computer network, every third party must secure its own connected systems in a manner consistent with HMS requirements. Harvard Medical School reserves the right to audit the security measures in effect on third party connected systems without prior warning. Harvard Medical School also reserves the right to immediately terminate network connections with all third party systems not meeting such requirements.

VI. Encryption

Default Protection Not Provided: HMS networks as well as the Internet and other public networks are not protected from wiretapping by default. In all but a few rare instances, if information is to be protected, then the User must take specific action to enable encryption facilities. Thus Users who employ cellular or mobile phones must not discuss sensitive (Confidential or Highly Restricted) information unless they have taken steps to encrypt the call. Likewise, videoconferences should not involve discussion of sensitive information unless encryption facilities are known to be enabled.

When To Use Encryption: Whenever sensitive (Confidential or Highly Restricted) information is sent over a public computer network like the Internet, encryption methods authorized by the Information Technology Department must be used to protect it. Whenever Highly Restricted information is stored in a computer, this storage must be achieved with similar authorized encryption methods.

Key Selection: Many encryption routines require that the User provide a seed or a key as input. Users must protect these security parameters from unauthorized disclosure, just as they would protect passwords from unauthorized disclosure. Rules for choosing strong seeds or keys should likewise follow the rules for choosing strong passwords (described in the section entitled Choosing Passwords).

See section XXV for policy governing the mobile device encryption policy.

VII. Electronic Mail

Sharing and Forwarding: Electronic mail accounts, like user-IDs, are for specific individuals and must not be shared. If a User goes on vacation or deems necessary for other reasons, mail can be forwarded or to another person or another individual may be delegated rights to access and send on the user's behalf without sharing user credentials. Likewise, notices can be established which will automatically notify correspondents that the recipient will not be responding for a certain period of time. Upon departure from Harvard Medical School, a User's electronic mail account must be terminated. To restrict the dissemination of sensitive information, no automatic forwarding of electronic mail to addresses outside Harvard Medical School is permitted unless authorized by HMS IT. If an electronic mail message contains sensitive information, Users must not forward it to another recipient unless (1) the other recipient is authorized to view the information, or (2) the originator approves the forwarding. The use of the blind carbon copy feature in electronic mail systems is discouraged because it is inconsistent with the open and honest communication at Harvard Medical School. Broadcast electronic mail message facilities should not be employed unless department manager approval is first obtained, but the use of selected distribution lists is both advisable and permissible without such approval.

Default Protection: Electronic mail is not protected from prying eyes by default. Electronic mail is the equivalent of a post card. Accordingly, Users must be careful about the inclusion of sensitive information in electronic mail messages that are not protected by encryption. To protect information from unauthorized disclosure, Users should employ encryption.

Message Recording: By default all electronic mail messages are recorded in logs and back-ups. This means that even though an electronic mail message may have been deleted from a User's in-box, it may still be retrievable with other methods.

Contents of Messages: Users must not use profanity, obscenities, or derogatory remarks in any electronic mail messages discussing staff, faculty, students, or others involved with Harvard Medical School business. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. Special caution is warranted because back-up and archival copies of electronic mail may actually be more permanent and more readily accessible than traditional paper communications.

VIII. Viruses and Malicious Software

Virus Checking Required: Virus checking systems approved by the Information Technology Department must be in place on all personal computers with operating systems susceptible to viruses, as well as on all firewalls with external network connections, and on all electronic mail servers. All files coming from external sources must be checked before execution or usage (if encryption or data compression has been used, these processes must be reversed before the virus checking process). Users are not authorized to turn off or disable virus checking systems.

If A Virus Is Detected: If Users obtain virus alerts, they must immediately disconnect from all networks and cease use of the affected computer, and then call the Information Technology help desk and get technical assistance. To prevent possible damage to Harvard Medical School information and information systems, Users are not permitted to remove viruses on their own. If Users believe they may have been the victim of other malicious software such as a Java applet, they must immediately call the Help Desk to minimize the damage. User possession or development of viruses or other malicious software is prohibited.

Spyware: Users should employ Spyware scanning software on any HMS workstation systems. Such Spyware scanners should be run at least monthly in order to assuage the proliferation of Spyware and malicious software.

Refer to section XII for information on how HMS IT deals with infected machines.

IX. Personal Use of Information Systems

Personal Use: All User activity is subject to logging and subsequent analysis. Users must not perform any activity on Harvard Medical School information systems which could damage the reputation of Harvard Medical School. Unbecoming conduct could lead to disciplinary action including revocation of access control privileges. Incidental personal use of Harvard Medical School information systems (including the telephone) is permissible so long as the usage does not interfere with job performance, does not deny other Users access to the system resources, and does not incur significant costs. Personal use of Harvard Medical School information, such as a mailing list, requires the advance approval of the relevant information Owner. Use of software licensed to Harvard Medical School on a personal computer owned by a User is not authorized unless the system has been designated a "system which is used to process Harvard Medical School information".

Testing Prohibition: Users must not test, or attempt to compromise any information security mechanism unless specifically authorized to do so by the Information Technology Department. For example, Users must not attempt to compromise anti-copying mechanisms built into commercial software. Users are prohibited from possessing software or other tools which are designed to compromise information security (for example, password cracking software). Any attempts to access any system in this manner will result in the offending machine's removal from the network.

X. DMCA (Digital Millennium Copyright Act)

Harvard Medical School complies with the Harvard University DMCA policy which can be viewed at <http://dmca.harvard.edu>.

In the event that a complaint is received by the HMS Security Officer, the offending system is traced and removed from the network. The HMS Client Services Group as well as the System Administrators are notified in the event of a staff/lab machine. The student helpdesk is notified in the event that a student machine is involved.

Once the offending machine is found, the materials specified in the infringement complaint must be removed either by the user or a CSR (Client Services Representative) or a System Administrator.

The user's information must be sent to the HMS Security Officer prior to the system being allowed back onto the network. The Security Officer sends out a notice of complaint to the user and reports their information to the central DMCA office in Cambridge.

About the DMCA:

The Digital Millennium Copyright Act (DMCA) was enacted to protect the intellectual property of individuals whose copyrighted works have been digitized and made available on the Internet.

All Harvard users must respect the copyrights in works that are accessible through computers connected to the Harvard network. Under federal copyright law, no copyrighted work may be copied, published, disseminated, displayed, performed or played without permission of the copyright holder. This includes music, movies and other copyrighted material.

Harvard may terminate the network access of users who are found to have repeatedly infringed the copyrights of others. Students with questions about copyrights or this policy are invited to raise those questions with any dean, tutor or academic officer. Staff supervisors and members of the Faculty are welcome to call the University's Office of General Counsel.

Complete information on the University's DMCA compliance policy can be found at Harvard University's Digital Millennium Copyright Act web site

XI. Peer to Peer File Sharing (P2P)

Peer-to-peer (P2P) file sharing applications are used to connect a computer directly to other computers in order to transfer files between the systems. Frequently such applications are used to transfer copyrighted materials such as music and movies.

In order to comply with the letter and intent of the University DMCA policy (<http://dmca.harvard.edu>), Peer-to-Peer applications are restricted on the HMS network, the HMS wireless network and the HMS VPN.

Examples of P2P applications are BitTorrent, Gnutella, Limewire, eMule and Ares Galaxy. Of these applications, BitTorrent has value in the scientific community. If your work requires the use of BitTorrent, an exception may be made for your system. A request for an exemption may be made by submitting a support request form or by contacting the HMS IT Help Desk at 617-432-2000.

To stem the use of P2P applications, HMS IT blocks well-known P2P ports. However, some applications will still negotiate connections on dynamic ports. If a system is detected engaging in P2P activity on the wired network, a temporary second level block is put in place on that system which shuts down the P2P

traffic. A notice is then sent out to the Quad System Administrators as well as the IT Client Services Group. The system identification is then logged.

If a particular system is blocked several times, it will be removed from the network until such time as the user uninstalls the offending software or states that they will not use it on the HMS Networks. Systems owned by HMS will have the software removed unless it is deemed necessary for the transfer of scientific data or other such valid use.

If a system engages in P2P traffic on the HMS Wireless network, that system is promptly removed from the wireless network as it is a clear violation of the acceptable use policy that the user is forced to agree to in order to use the wireless network.

If a user engages in P2P activity while connected to the HMS network via VPN, the user is identified and notified by email that this is a violation of the acceptable use policy. Continued use of P2P application over VPN may result in the termination of VPN access.

HMS IT is not always successful in preventing the use of these applications. Occasionally a DMCA violation notice is registered with the University DMCA Office regarding an offense. Typically these offenses are the result of a user sharing copyrighted materials.

When a DMCA violation notice is received, the offending system is immediately removed from the network pending a further investigation. Once the user is identified an official notice is sent from the HMS Security Officer. The user's information is sent to the University DMCA office and is kept on file.

In the event of a second offense the user is restricted from using the HMS Network for the period of one year. If the user requires the use of the HMS Network for their job, this may result in termination.

XII. Compromised Systems

When a machine is suspected of having been infected or compromised, the system is tracked down by MAC address to the switch that it is connected to. The switch port is then disabled and the MAC address is added to an exclude list on the DHCP server (if the device uses a non-static IP address). This prevents the device from obtaining an IP address should the user plug the device into a different jack.

Any system that likewise causes performance issues or denies services shall be removed from the network and also from DHCP.

An email is then sent to the `it_staff@hms.harvard.edu` and `hms-sysadmins@hms.harvard.edu` groups in the event of a staff network or to the Student Computing group in the case of a student machine, notifying them that the system has been removed.

In certain cases a security scan is run against the offending machine in order to attempt to determine what vulnerabilities may exist, if any. This helps to eliminate false positives.

Suspicious devices are identified through a combination of a perimeter IDS (Intrusion Detection System), firewall logs, and other tools.

XIII. DMZ

The DMZ (or screened subnet) is a separate network that exists off of the perimeter firewall. The DMZ is used for servers that require that they be accessed from the outside world while at the same time can be

limited to the communication required inside of the network. SMTP and WWW servers are a perfect example of this. Exceptions are made based upon the following criteria:

1. Does this machine need to be backed up?
2. How many ports need to be open from the DMZ to the internal network if the device were on the DMZ?
3. Is the machine a workstation or server?

Depending on the answers to the above, the DMZ may not be the ideal place for the device. In such a case, an exception is made to allow traffic into the internal network. See Firewall Request below.

XIV. Public V. Private IP space

HMS IT is in the process of getting all workstations (and a majority of servers) to use private IP space. All new devices requiring a static IP address will be issued a private IP address unless the below conditions are met.

The criteria for a new device to receive a public IP address are as follows:

1. Does the machine need to be accessed from outside of the school.
 - a. This may involve the machine being placed on the DMZ, however this is not always logistically feasible. These are handled on a case by case basis.
2. Does the machine need to connect to another institution via VPN.
 - a. Some VPN implementations break when the client uses NAT (Network Address Translation). In these cases, a public IP address must be used for the client.

There may be other examples where public IP addressing needs to be used. If the rationale is not clear cut, then it is handled on a case by case basis.

XV. Firewall Permissions

By default, any traffic initiated from the outside of the network is blocked. Traffic originating from the inside is allowed outbound without restriction. Traffic that needs to be allowed into the network is opened specifically based upon the criteria below.

XVI. Firewall Requests

All firewall requests are to be made through the IT ticketing system. Firewall requests must be reviewed against current security practices prior to being approved by the Information Security Officer or other members of the HMS IT networking group. In some cases additional system administrators must be involved in the decision to make a firewall change, specifically to the internal firewall that protects more sensitive data. Approved changes are made Monday through Thursday. **Firewall changes are not made on Fridays or on the day prior to a holiday break.**

Firewall requests will only be honored when made by authorized personnel. The Security Analyst/Firewall Administrator will only honor requests made by system administrators who are directly responsible for the systems for which access is being requested.

When requesting a firewall exception the following information is required to appear in the ticket:

¹Source IP address, Destination IP address, Port/Application (TCP/UDP)

In the event that traffic from outside the school is being allowed in, the following guidelines are followed:

1. Protocols allowed should be encrypted if possible.
2. Access should be restricted to a subset of IP addresses. This determination is based upon the audience. In the case of a web server, access from the world is generally accepted.
3. Remote administration services are not allowed. Applications such as VNC, PCAnywhere, etc. are not allowed through the firewall. If remote administration is required the user will be issued a VPN account.
4. New servers should be placed on the DMZ when feasible, as well as any system that needs to be access from outside the school without using VPN. See above DMZ Guidelines.
5. Because of the ubiquitous nature of Microsoft's operating systems and the associated number of vulnerabilities and exploits, Harvard Medical School does not allow Microsoft RPC (Remote procedure call) protocols through from outside of the school network.

XVII. Internal Firewalls

Harvard Medical School uses internal firewalls to protect certain more sensitive systems from the rest of the campus network. Access to these devices is requested by the owners/managers of each device. An example of this would be the Windows MED Domain. The MED domain is a Microsoft windows domain that is maintained by the Operations group within Networking Operations. All access requests for the domain controllers and file servers must either be made by or approved by the Operations group.

XVIII. Wireless Security

The HMS Wireless network utilizes an encrypted authentication process in order to get access. Once authenticated, traffic is not encrypted by default. The HMS Wireless network is to be used for non-sensitive, lightweight applications. Users of the HMS Wireless network are strongly discouraged from using it for any credit card or financial data.

Users wishing to have their connection encrypted once on the wireless network should use the HMS VPN solution, which provides a 168bit 3DES encryption algorithm.

¹ Source and destination IP addresses must be static

Harvard Medical School Wireless Access Security Guidelines

Introduction:

The HMS wireless network is available to any HMS employee, student or HMS affiliate who possesses a valid UTAG approved login ID and password. The use of the wireless network must not reduce the availability, integrity and confidentiality of critical and essential applications of the HMS computer network. Accordingly, the implementation of the wireless network systems should comply with the security standards established by the HMS Network Security policies for authentication, monitoring, reporting and user awareness.

Disclaimer:

The HMS wireless network is operated without encryption in order to foster the sharing of information between different Harvard University campuses. Therefore, there is no reasonable expectation of privacy while using the HMS Wireless Network. Most traffic is sent in “in the clear” and can be watched by other machines. Harvard Medical School neither implies nor guarantees any level of privacy of data or communications while using the wireless network.

Authentication for the HMS Wireless Access:

Authentication is done through a web browser with SSL encryption. The wireless network authentication follows the guidelines established by the Harvard University Technical Architecture Group (UTAG) for the wireless networks at Harvard University.

These guidelines include the following:

- Web Browser Enabled Authentication
- Common look and feel among all Harvard Schools
- Does not require installation of software clients on the user’s devices

As a part of these guidelines, the wireless network uses the following authentication mechanisms in order to foster collegial atmosphere throughout the disciplines of the University.

Valid HMS eCommons ID
Harvard University PIN
SPH credentials
KSG credentials

Authentication Timeout Policy for the HMS Wireless Network:

Because of the security concerns inherent with the wireless network, the HMS Information Technology Department has defined an authentication timeout period of 30 minutes. HMS wireless users have to authenticate again if their devices are idle for more than 30 minutes.

Harvard Medical School Wireless Network Acceptable Use Policy:

The wireless network use is strictly for HMS, HMS Affiliates, students, faculty and staff. Unauthorized use of this wireless network is prohibited. All wireless users agree to abide by the **Wireless Acceptable Use Policy** as defined below. The HMS IT Department reserves the right to terminate the wireless network connection of those who are in violation of this policy.

Wireless is appropriate for “common areas” where Students, Staff, and Faculty gather. Common areas most appropriate for wireless are conference rooms and auditoriums.

Wireless networking is most suitable for applications that require low bandwidth such as email and web surfing. High bandwidth applications on the wireless network may impact other users. Please refrain from using them. The wireless network is an augmentation and not a replacement of the wired network extending the network for general purposes to common and transient areas. Wireless users should be aware the user accounts, passwords and wireless network interface cards (NIC’s) are not to be shared.

Unless using encrypted protocols wireless devices should not be used for connecting to campus business systems such as human resources, payroll and student information, financial information systems or other systems that contain sensitive information or are critical to the mission of the University.

Wireless users should be aware that the wireless client computers are not appropriate to run as servers. Any device that impacts the wireless network performance will be removed.

XIX. Networking Device Policy

Executive Summary

HMS Networking provides high-speed network services. In order to protect the network, while meeting the needs of the HMS community, there are policies in place that restrict the use of network devices like hubs, switches, routers and wireless access points. Such equipment can cause real security threats and can lead to loss of service across the network if improperly configured or compromised. HMS departments should follow these policies. HMS Networking can, however, work with users to accommodate their particular and often unique needs in a way that is secure and preserves the quality of the network. If someone has the need to install these devices then they should work in consultation with HMS Networking to determine the optimum solution for the user and the network. This document provided technical background and official policy guidelines for HMS.

Introduction:

HMS Networking provides a high-speed network that is secured at the perimeter and also secures more sensitive services behind an internal firewall. Entry to this network is controlled via a secure IPSEC VPN solution. Wireless access is controlled via an authentication service that helps to protect the network from unauthorized admittance as well as encrypting the login process to protect user credentials.

It is very easy for user-configured wireless access points, hubs or switches to represent an open and unauthenticated entry point into the Harvard Medical School network; one that circumvents HMS Information Technology architecture standards and best practices for protecting the HMS Network and for maintaining standards of performance.

Unlike hubs and switches, wireless access points do not require an unauthorized user to be located physically on campus. A user outside of or adjacent to the campus may be able to eavesdrop on wireless communications.

Additionally these unauthorized devices may degrade network performance and cause a denial of service if not properly configured. Installation of these devices is not in keeping with current infrastructure standards and serves to undermine the capital investment that Harvard Medical School has made in the Information Technology infrastructure of the campus.

The HMS data network is a resource that enables HMS staff, faculty, researchers and students to conduct the businesses of education and science. As such, the HMS data network is a resource that is shared by the community and is an important part of the work that is done by the University, the faculty, staff and affiliates. Installation of unauthorized devices may adversely impact other users on the network and reduce the ability of the University to conduct the businesses of education and science.

Wireless Access Points:

Unauthorized wireless access points arguably have the greatest potential for granting unauthorized network access. HMS networking in conjunction with UTAG (University Technology Architecture Group) has developed a method to securely authenticate users of the HMS wireless quad. This authentication helps to insure that only authorized users have access to campus network resources.

Unauthorized wireless access points do not use this secure authentication, potentially allowing unauthorized users access to University and laboratory resources. Unlike common data jacks, wireless access points open holes in the network that are not restricted to a physical on-site location. A wireless access point may allow users from other neighboring institutions, apartment buildings, parked cars, retail establishments, etc. access to the Harvard Medical School network and information resources without a username/password challenge or any encryption. An Unauthorized access point may also create channel interference and impact the performance of the HMS Wireless network.

The only authorized access points are those that are installed by or authorized by HMS IT and conform to the UTAG standard for authentication.

Policy Summary:

- I. HMS Networking does not permit the use of user installed wireless access points. Use of such devices constitutes a breach of network security and violates the HMS networking architecture.
- II. When a wireless access point causes a denial of service or adversely impact the performance of the HMS Network, HMS Information Technology will work with the user to remove the device from the network with the least disruption to their operations. If HMS cannot quickly locate the user and other users are affected the network connection for the device will be immediately disabled. The user will be cautioned not to put unauthorized devices onto the HMS Network. If the device is found to have been placed back onto the network, HMS IT will remove the device from the network and work with their departmental administration to ensure that they do not persist in the practice.
- III. Users desiring wireless access must contact the Harvard Medical School Networking group through the HMS Helpdesk and begin a review process with the wireless implementation team. The wireless team will assess the need for and provide costs for implementing an authenticated secure wireless implementation. The wireless access point(s) that would be installed as a result of the implementation process would be one(s) that conforms to the HMS standards for security and network architecture. HMS Networking can work with the user to install such equipment.
- IV. If an unauthorized or “rogue” access point is discovered the following actions will be taken:
 - a. **Initial discovery** – Because of the inherent security issues associated with wireless access points, unauthorized devices must be removed from the network as quickly as possible upon detection. Notification will be sent to the HMS-Sysadmins@hms.harvard.edu and IT_Staff@hms.harvard.edu mailing lists and directly to local administrators, if known. HMS Networking will work with the user to find an adequate and secure solution for their needs. If, however, there is any evidence that the device is affecting other users HMS Networking will remove or deactivate the device immediately. It is recommended that the device be removed during this process while a solution is being examined.

- b. **Second discovery** – If an access point is found to have been put back on the network after initial removal HMS IT will remove the device from the network and work with the local department management to resolve the issue.

Networking Devices:

Unauthorized networking devices are in violation of the HMS Networking groups standard of providing excellence in data connectivity. HMS Networking provides an enterprise level high speed switched networking environment. The HMS data network has been designed and built in order to foster collaboration in a safe and expedient environment for education and research. HMS Networking recognizes that the heterogeneity of research at HMS means that exceptions are needed – HMS Networking will work with the user(s) to provide a solution that is both performance and security driven.

Installation of unauthorized network devices can impact the performance of the network to the end user. Some devices use shared technology and may result in several users sharing an amount of bandwidth that would normally be dedicated to a single user.

Installation of networking devices places appliances onto the network that are beyond the control of the HMS Networking group and therefore makes troubleshooting any issues more complicated if not impossible based on the level of disclosure from the client.

Users desiring additional data connectivity must contact the HMS IT Helpdesk and submit a request for data jack installation.

In the event of an infection or hack, HMS information security disables the port on the switch of the infected machine. If an unauthorized device is in use, all machines connected to the device will also lose their connections.

Policy Summary:

- I. HMS Information Technology does not allow any networking device to be placed on the network by anyone other than the staff of HMS Networking unless reviewed and approved by HMS Networking. The use of unauthorized hubs, switches, and other networking devices is expressly prohibited. Use of such devices constitutes a breach of HMS IT architectural standards.
- II. Additional data connectivity is provided by IT through the installation of data jacks. Users may request the installation of additional jacks through the HMS IT Helpdesk.
- III. If an unauthorized networking device is found, the following actions will be taken:
 - a. **Initial discovery:** The user will be notified and given a four week grace period in which to order additional data jacks or work with IT to find an alternate solution. Notification will be sent to the HMS-Sysadmins@hms.harvard.edu and IT_Staff@hms.harvard.edu mailing lists and directly to local administrators, if known. HMS Networking will work with the user to find an adequate and secure solution for their needs. If, however, there is any evidence that the device is affecting other users HMS Networking may remove or deactivate the device immediately.
 - b. **Second discovery** – If a network device is found to have been put back on the network after initial removal HMS IT will remove the device from the network and work with the local department management to resolve the issue.

Remote Access Devices (Dial-in Servers):

Harvard Medical School provides a VPN solution for secure access to the network. This access is controlled and maintained by IT utilizing central authentication services. Accounts are maintained in conjunction with the HR Core database in order to disable accounts of terminated staff, to disable the accounts of students who have graduated and to create accounts for new users in a timely fashion.

Permissions for the VPN network are separate from the internal networks and access for certain highly sensitive services is restricted by default. Exceptions are made on a per request basis based on business or academic need.

Policy Summary:

- I. HMS IT does not allow dial-in devices to be present on the HMS Network. The use of dial-in devices is expressly prohibited. Use of such devices constitutes a breach of HMS IT architectural standards
- II. Users requiring remote connectivity must request a VPN account through the HMS IT Helpdesk. A standard Internet connection is required in order to use the VPN solution.
- III. If a dial-in device is discovered on the network the following actions will be taken:
 - a. **Initial discovery:** The user will be notified and given a four week grace period in which to obtain VPN accounts for users. After this time, the device will be removed from the network.
 - b. **Second discovery:** If a dial-in device is found to have been put back on the network after initial removal HMS IT will remove the device from the network and work with the local department management to resolve the issue.

Summary:

HMS IT strives to provide the best possible data network performance and security to all members of the HMS community. In order to provide a consistent level of service performance and security, HMS IT must manage all networking devices that use the HMS data network. Therefore, HMS IT prohibits the placing of unauthorized devices onto the network.

Requests for authorization, as with all requests, should begin with the IT Helpdesk at extension 2-2000 or by email at help_desk@hms.harvard.edu.

Unauthorized devices pose a significant risk to not only the performance but to the security of the network and the devices attached. The HMS data network is maintained for the use of all students, staff, faculty, researchers and affiliates. Installation of unauthorized devices may negatively impact others abilities to do their work and may result in the loss or theft of sensitive information.

Circumstances may arise such that a “stop-gap” measure would be required in order to provide data connectivity outside of the course of the existing infrastructure. HMS IT should be consulted prior to the installation of any device onto the network. HMS IT will review and, if possible, install a temporary solution. If this is not possible because of time or staffing limitations, HMS IT will grant a temporary waiver for the installation of a temporary solution.

Certain “out-of-band” networks may be set-up if approved by the HMS Networking group. These networks are typically used for data backups. HMS IT does not support any non-standard networking gear. Installation of supported networking devices can be coordinated through the HMS Networking group. Installation of any networking device should be coordinated through the Net-Ops group for proper IP address assignment.

XX. HIPAA – Health Insurance Portability and Accountability Act of 1996

HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996. The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing various unrelated provisions of HIPAA, therefore HIPAA may mean different things to different people.

Above all, HIPAA addresses the security and privacy of health data. HMS is not a HIPAA Covered Entity; therefore there is no formal audit of our systems to ensure protected healthcare information is secure. Hence, HMS systems should not be used to store protected healthcare information.

HMS Information Technology may not be held accountable for any patient data stored on the HMS Network.

XXI. Technology Resources Utilization

It is every User's duty to use the HMS IT resources responsibly and in a professional, ethical, and lawful manner. In addition, every User is responsible for ensuring the security of the HMS IT resources and its valuable proprietary and confidential information.

Users have a responsibility to insure that their desktop systems are in compliance with the latest operating system and applications patches. All Users should have the auto-update feature enabled for patch integration. Systems that have several high-risk vulnerabilities may be removed from the network in order to protect the integrity of the remaining systems.

All systems connected to the HMS Network must be running Anti-Virus software and be up to date for virus signatures.

XXII. Backup Data

Harvard Medical School Information Technology uses a secure vendor for the storage and indexing of system backup data. The HMS IT Backup rotation is somewhat dynamic in nature and has no fixed length of time for retaining data. Some backups may be retained indefinitely while other may be kept for a short time only.

Once backup media has been retired, the media is sent to the vendor for secure destruction. Once destroyed a certificate is sent back to HMS IT stating that a certain number of media were destroyed.

XXIII. Remote Access

Individual employees and departments are responsible for any Harvard information accessed remotely or stored on remote access devices. Individual employees and departments are responsible for any information deemed to be personal information, as well as any high-risk confidential information access remotely.

Obtaining Access

Harvard Medical School provides basic remote access to qualified users. Basic access consists of the services granted through the HMS SSL VPN portal page at secure.med.harvard.edu. These basic services are limited to web based access to web-enabled services and storage.

Greater access, such as Terminal Services and Network Connect are granted on a per request basis for qualified users.

Working Remotely

Users who access the HMS network remotely must do so with a computer that is up to date for operating system patches, anti-virus software and anti-spyware software. Systems should have automatic updates enabled and be regularly scanned for malware. Anti-virus/Anti-spyware software should be set to automatically protect the remote system and not be disabled in any way.

Users must ensure that any confidential information is stored on a server or other HMS device, such as centralized storage, unless the remote device is properly encrypted. Users are responsible for maintaining the security of any personal and confidential information that is stored on a remote device.

University Policy expressly prohibits users from storing any High Risk Confidential Information on any remote device, mobile media or any system other than an HMS centralized server or storage system. Exceptions may be made on an as-needed basis. The Harvard Medical School CIO must approve these exceptions.

The form to request an exemption may be found at:
<http://www.security.harvard.edu/resources/forms>

HMS Information Technology may, at any time, terminate, suspend or otherwise restrict access through the HMS VPN for any violation of the HMS acceptable use policy or if the behavior of the system connected suggests any infection by malware or malfeasance on the part of the user.

In keeping with Information Security best practices, the HMS VPN does not split-tunnel the connection. All Internet bound traffic will traverse the HMS network and is, therefore, governed by HMS policy.

Invited User Remote Access

HMS provides remote access for consultants, contractors and other classes of workers who require access to HMS resources but do not qualify for full access. In these cases, each user must have an HMS sponsor. The sponsor may request access via the HMS Invited User Request form, found on the HMS Information Technology website.

If a VPN account is requested, a follow-up VPN request ticket is generated for the HMS Information Security group. HMS Information Security will then contact the sponsor and provision a VPN account to access a resource or resources that are specifically requested. Only access that is specifically requested will be granted. Whereas the connection is not split-tunneled, this applies to Internet access as well.

XXIV. Confidential Information

Confidential Information is information about a person or an entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk of criminal or civil liability, or be damaging to financial standing, employability, or reputation. Harvard is bound by law or by contract to protect some types of confidential information. Additionally, Harvard requires protection of some other kinds of information beyond legal or contractual requirements as an additional safeguard.

Confidential Personally Identifiable Information

Confidential Personally Identifiable Information includes information that can be linked, directly or indirectly, to individual people. Harvard's requirement to protect confidential personally identifiable information is largely governed by law or contract, (e.g. HIPAA, FERPA, GLB, PCI, and human subject data). Examples include Social Security Number, Harvard University ID, credit card, health and employment records, human subject data, and all FERPA non-directory information about students and former students.

Confidential Non-Personally Identifiable Information

Confidential Non-Personally Identifiable Information includes summary information about people where the identities of individual people cannot be determined and information about university-related activities. Harvard's requirement to protect confidential non-personally identifiable information is governed by Harvard's own policies. Examples include detailed information about some University buildings, activities or events, information about future University development plans, and grant information.

Guidelines

Accountability and Security

All information gathered and maintained by the staff for the purpose of conducting University business is considered institutional information, and as such, each staff person who uses, stores, processes, transfers, administers and/or maintains this information is responsible, and should be held accountable for its appropriate use. Responsible parties and proper security measures should be established to protect user files and system resources from loss, damage, inappropriate access and unauthorized disclosure.

Controlling Access

Before being given access to sensitive information, individuals should be trained in the importance of protecting sensitive information from being disclosed. While gathering information as required by job responsibilities, staff should make reasonable attempts to prevent disclosure. Access to confidential information and to systems containing confidential information should be confined to staff that need to know, and must be controlled by a process that meets the following criteria and characteristics:

- Access to the University's administered systems (e.g. Oracle, Peoplesoft, Harvard Data Warehouse, etc.) should be restricted to those individuals who require it as part of the job description.
- The Harvard PIN Server is to be used for all applications at Harvard that access confidential information.

- Confidential information, ID's and passwords transported over a network must always be encrypted.
- All access must be by individuals who identify themselves uniquely to the systems.
- A combination of a login name and a secret password that is known only by the user, or a combination of a login name, a secret password that is known only by the user, and a piece of data generated by an electronic device in the possession of the user (e.g. a SecureID card).
- HMS recommends the following guidelines for passwords that are used to access systems containing confidential information:
 - Never give your username, password, or PIN to anyone else
 - Never use someone else's user name, password or PIN
 - Do not use easy-to-guess passwords or PINs
 - Be aware of those around you to ensure they can't watch you typing your passwords or PIN
 - Do not write down passwords or PINs
 - Do not allow others to access programs or data from within your account.
 - Change your password often
 - Log off your workstation when leaving for the day
 - Lock your workstation when leaving the area
 - Do not use your University password with external vendors

For more information on controlling access, please go to the [Harvard Risk Management and Audit Services Web Site](#).

Information Handling

Staff must take special care when transporting, storing, displaying and disposing of confidential information regardless of the data form.

Electronic Information

Electronic information is at particularly high risk due to the ease of transport. Staff should take the following precautions when dealing with confidential information electronically:

Computer Systems

Staff should ensure that the software on their computers is secure and the machines are operated in a way to minimize the chance of a security breach. All computers used to access Harvard confidential data must have DLS approved anti-virus, Internet security and firewall software applications.

Data transmission

Precautions should always be taken when transmitting information electronically.

- Electronic mail (email) may, in some situations, be considered an insecure mechanism for exchanging information. The confidentiality of information contained within e-mail messages can be exposed, especially when either the sender or any of the recipients are off-campus or utilize a wireless network connection.
- Special care should be taken when selecting addresses or distribution lists to avoid unintended recipients from receiving the information.
- Salary information and ID information should not be transferred via email.
- When sending a fax, be sure that the correct number is dialed and that a cover sheet is always used.

Data Storage

No member of the Harvard community is permitted to store Social Security, credit card, or bank account numbers in any way relating to Harvard or Harvard sponsored activities on any user computer. This information must be stored on protected servers or secure shared file systems. This rule applies to all desktops and laptops, whether the computer is owned by Harvard or not, and whether the data is encrypted.

Data Disposal

Destruction of information on computer disks and other magnetic formats should be done with an overwriting process that meets Federal Guidelines. Simply “erasing“ the data is not sufficient to completely destroy the information, resulting in potential recovery and disclosure. Hard disk drives or other data storage systems may require physical destruction.

Display Screens

The display screens for PC’s and workstations used to view or process sensitive information should be positioned such that those who do not have access cannot view them. A password-protected screensaver should be activated on your computer to ensure your system is secure when away from your work area.

Testing and Training

The University maintains additional environments for development in which institutional data is retained. Precautions should be taken when testing or training on systems that contain sensitive information. Application system developers and installers shall provide user training on security issues when new Systems are installed. Copies of production Data should not be used for purposes that may compromise the confidentiality of individuals or organizations.

Physical Documents

When handling physical documents containing sensitive information, steps should be taken to safeguard the information from disclosure. Below are some HMS recommended guidelines for handling documents containing sensitive information:

- Documents should be clearly stamped “confidential” and/or “Do not copy or distribute”
- Documents should be stored in a secure location (e.g. room, file cabinet, etc.) to which only specifically-approved individuals have access through lock and key at all times
- Never leave extra copies of handouts in conference rooms or other public areas
- When printing to a public printer, be sure to retrieve documents immediately
- Documents must be shredded using a university-approved device or shredding facility prior to being discarded

Verbal Information

When discussing sensitive or confidential information with other individuals either within or outside of the University, HMS recommends the following guidelines:

- Staff should not verbally disclose confidential information to individuals outside of the University (e.g. vendors or peer institutions) except as authorized when obtaining quotes, purchasing, benchmarking or doing research.
- When passing information to individuals outside of the University, staff should ensure that the recipient understands that they cannot disclose or utilize the information in a way that is inconsistent with the intended use.
- When communicating confidential information to others within the organization, staff should make sure that these conversations only take place in areas where unintended recipients cannot overhear information.
- When a telephone speakerphone is used during a phone conversation, staff should make sure that all participants in the conversation know that a speakerphone is being used and are informed of each participant in the room. Speakerphone meetings should only take place in an office or conference room with a closed door so that remote participants in the meeting can be ensured of the confidential nature of the conversation.

Obtaining Confidential Information

The use of high-risk information in local business processes is discouraged. When required, it must be used only with approval of the CIO. Existing applications that use high-risk information at present are subject to annual review for re-certification.

Forms are provided at the following location in order to request HRCI and other confidential information:
<http://www.security.harvard.edu/resources/forms>

This approval process for requesting high-risk confidential information must be completed as a prerequisite and updated annually.

1. The requester must document the purpose for which the information is being requested. The description must include sound justification.
2. The requester must document the additional protections that will be employed to keep the high-risk information secure. These protections must be in accord with the Enterprise Security Policy.
3. When the business purpose, justification, and protection description have been documented, the requester must send this to the approver of the data source from which the information is requested.
4. The approver will review the request, indicate whether this is an existing data transfer, and will forward to the University Technology Security Officer (UTSO).
5. The UTSO will review and work with the requester to obtain additional information or to clarify the request if needed.
6. The UTSO will send the request, along with a recommendation, to the CIO for review and a decision to be made after consultation by the CIO with the appropriate Vice President and relevant business leaders.
7. The CIO will inform the UTSO of the decision and will retain a copy in the CIO's files for future reference and annual review of approved requests.
8. The UTSO will inform the requester and the data owner about the outcome of the request. If the CIO has approved it, the requester may then initiate the process for requesting the information.
9. If a request for high-risk data is approved, the requester must arrange for a system audit through Harvard Risk Management and Audit Services (RMAS) prior to receiving access to high-risk data.

XXV. Mobile Device Encryption

Laptops

All University owned laptops must be protected with whole disk encryption (WDE). Note that the University considers any laptop purchased with a grant to be University owned as well as laptops that are purchased through normal procurement methods. High Risk Data must only be stored, when absolutely required, on University owned systems with WDE. The HMS CIO must approve the storage of all HRCI on any system other than a centrally managed server or storage system.

HMS offers PGP Whole Disk Encryption as a WDE solution for Windows and OS X systems. Users may choose to install the WDE client as a stand-alone solution or to participate in the HMS Enterprise WDE deployment. The benefit to participation in the enterprise solution is that HMS Information Technology will be able to unlock an encrypted drive should a password be forgotten or lost.

Users may also use the BitLocker WDE built into Windows Vista Ultimate or Windows 7 Ultimate editions. Please note that Apple File Vault encryption does not meet the standard, as it does not encrypt the entire hard disk, only the user's home directory. Thus, File Vault may not be used as a suitable substitute for PGP WDE.

As with any stand-alone installation, HMS Information Technology will be unable to unlock the disk should a password be lost or forgotten.

HMS Information Technology will be rolling out the PGP WDE product to systems that are known to deal with High Risk Confidential Information. All other users are encouraged to contact HMS IT to arrange for installation.

In order to obtain copies of PGP WDE, please contact the HMS Information Technology Help Desk at (617) 432-2000 or by email at help_desk@hms.harvard.edu

Smartphones/PDA's

All smartphones (Blackberry, iPhone, Pre, etc.) and personal digital assistants (PDAs) must require a Personal Identification Number (PIN) be entered in order to use the device. The device must be set to lock automatically after a period of 2 minutes and set to erase all data on the phone after a series of unsuccessful passwords. HMS IT recommends the number of unsuccessful attempts be limited to 10.

All email communication on smartphones must also be encrypted. The transfer of any personal information must be encrypted. All mobile devices that store personal information must be encrypted.

HMS IT will force PIN use on Blackberry devices that are registered on the HMS Blackberry Enterprise Server (BES) and other smartphones that are connected via Active Sync.

HMS IT does not force encryption. Encryption of the device is the responsibility of the user.