Information Technology Policies

Policies Deprecated -- December 2018

Take me to Current Policies

USE POLICIES

A. INTRODUCTION

Information technology continues to expand in use and importance throughout The Johns Hopkins University ("JHU") and The Johns Hopkins Health System Corporation ("JHHS"), collectively "Johns Hopkins" and "JH." It is an indispensable tool for education, research, and clinical care, and plays a central role in the overall life of the Institutions. The uses of information technology have changed dramatically over the last twenty years, and it is likely that the rate of change will accelerate in the future. For these reasons, it is critical that Johns Hopkins articulate a clear statement regarding the appropriate uses of our information technology resources and institute safeguards to ensure that our technology is secure, reliable, and available for the entire Johns Hopkins community.

These Policies have three primary purposes:

1. To ensure compliance with all applicable federal, state, and local laws

2. To safeguard and protect all IT Resources from anything other than authorized and intended use

3. To provide protection to academic, clinical, financial, research, and all other systems that support the mission and functions of Johns Hopkins.

E-mail and user accounts and their contents are generally considered private by Johns Hopkins, but neither this policy nor present technology is able to guarantee security, privacy or confidentiality. It is not the routine policy of JH IT administrators to view or disclose the content of others' electronic files, but JH reserves the right, and may be legally required, to access, copy, examine, and/or disclose all files stored or transmitted on, across or through JH IT Resources, in a number of circumstances, including: for safety, security, and/or legal purposes; as needed to maintain or protect its personnel, facilities and not-for-profit status; as necessary to maintain network services; or in order to protect JH's rights or property. For these reasons, there should be no presumption of privacy or confidentiality concerning information stored on or transmitted across JH IT Resources.

Certain information (such as protected patient health information; sensitive information regarding students or staff; and other information protected by the attorney-client privilege) is protected by law, and persons with access to such information are expected to be aware of and comply fully with the laws protecting such information. Nothing in these Policies is intended to affect in any way the confidentiality or protection of such information.

Johns Hopkins complies fully with all federal, state, and local laws, including the Digital Millennium Copyright Act. Except as required for IT security and functionality, access for the JH community to resources through computer networks should be governed by the standards and principles of intellectual and academic freedom characteristic of a university. All legal questions should be directed to the JHU Office of General Counsel or JHHS Office of General Counsel for the respective entity, school, or department involved.

The *Use Policies* were approved by the ICSC, Chief Information Officer and Council of Deans in February, 2005. The *Technical and Security Policies* were approved by the ICSC, Chief Information Officer and Chief Information Security Officer in September, 2005 and revisions approved in November, 2006, April 2007, January 2010 and March 2013.

B. DEFINITIONS

Confidential – see below, *Electronic Information Classification Policy*.

Covered Personnel – faculty, staff, employees, students, volunteers, officers, trustees, guests, visitors, and other workforce members, such as casual workers, consultants, temporary staff, and vendors.

Internal Use-Only – see Policy 5 below, *Electronic Information Classification Policy*.

IT Resources – information technology ("IT") resources of Johns Hopkins, which include, but are not limited to host computers; file, application, communication, mail, fax, Web, and print servers; workstations; stand-alone computers; laptops; portable devices; printers; software; data files on machines and on other storage media; switches, routers, cables; and all other internal and external computer and communications resources. IT Resources acquired by Johns Hopkins are considered JH property.

Johns Hopkins and JH – are used interchangeably and each means and includes: The Johns Hopkins University (excluding APL); The Johns Hopkins Health System Corporation, which includes Johns Hopkins Hospital; Johns Hopkins Bayview Medical Center; Howard County General Hospital; Johns Hopkins Community Physicians; and all of the schools, divisions, departments, and affiliated corporations of any or all of these entities.

Network and JH Network – IT Resources inter-connected in order to provide IT services to the JH community. The JH Network is composed of both wired and wireless components that are connected using a variety of network resources. Examples of network resources are hubs, routers, cables, switches, and wireless access points.

Restricted – see below, *Electronic Information Classification Policy*.

Security Device – IT Resources that provide for the confidentiality, integrity and availability of the IT resources connected to the JH Network. Examples of Security Devices include vulnerability scanners, network firewalls, password crackers and network/server intrusion detection sensors.

Unrestricted – see below,

Electronic Information Classification Policy.

C. SPONSORSHIP

Johns Hopkins recognizes that each principal entity or division of Johns Hopkins operates with relative independence, and each such entity or division is encouraged to develop, maintain, and publish specific procedures and practices, including authorization procedures, to implement these Policies according to its own academic or business needs.

D. ENFORCEMENT

The failure by Covered Personnel to comply with these Policies may result in loss of access to some or all of IT Resources and/or loss of access privileges to IT Resources. In addition, violators of these Policies may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.

E. REVIEW CYCLE

These Policies will be reviewed at least every two (2) years.

USER POLICIES

1. USE OF IT RESOURCES

Acceptable Use

Acceptable use of IT Resources is use that is consistent with Johns Hopkins' missions of education, research, service, and patient care, and is legal, ethical, and honest. Acceptable use must respect intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation, harassment, and annoyance. Further, it must show consideration in the consumption and utilization of IT Resources, and it must not jeopardize Johns Hopkins' not-for-profit status. Incidental personal use of IT Resources is permitted if consistent with applicable JH and divisional policy, and if such use is reasonable, not excessive, and does not impair work performance or productivity.

Unacceptable Use

Unacceptable use of IT Resources includes, but is not limited to:

a. Unauthorized access to or unauthorized use of JH IT Resources.

b. Use of IT Resources in violation of any applicable law.

c. Harassing others by sending annoying, abusive, profane, threatening, defamatory, offensive, or unnecessarily repetitive messages or web-site postings, or by sending messages or web-site postings that appear to come from someone other than the sender.

d. Any activity designed to hinder another person's or institution's use of its own information technology resources.

e. Privacy violations (e.g., disclosure or misuse of private information of others).

f. Installation of inappropriate software or hardware on IT Resources (e.g., network or password "sniffing" software, offensive applications, and malicious software).

g. Any use of copyrighted materials in violation of copyright laws or of vendor licensing agreements (e.g. illegal downloading and/or sharing of media files or computer software).

h. Intentional, non-incidental acquisition, storage, and/or display of sexually explicit images, except for acknowledged, legitimate medical, scholarly, educational, or forensic purposes. Exposure and/or display of such material may be offensive, constitute sexual harassment or create a hostile work environment.

i. Security breaches, intentional or otherwise, including, as examples, improper disclosure of a password, use of another user's account, or negligent management of a server resulting in its unauthorized use or compromise.

j. Commercial use of IT Resources for business purposes not related to Johns Hopkins.

k. Use (e.g. e-mail, social media, blogs), without specific authorization, to imply JH support (as opposed to personal support) for any position or proposition.

l. Use to engage in activities, including for example certain political activities, prohibited to tax exempt 501 (c) (3) organizations or that otherwise may result in a hostile work environment.

2. E-MAIL USE

The JH e-mail systems are used to support Johns Hopkins' mission and to allow effective communication between faculty, staff, students, and business associates. These systems vary substantially in size, scope and sophistication. Policies and procedures regarding e-mail storage, back-up, and archiving also vary substantially across JH. In addition, there is no single e-mail archive system for the entire institution. Back-up, storage and archiving of important e-mail messages are the responsibility of each individual user.

E-mail transmission over the Internet is inherently insecure and subject to security breaches that include message interception, message alteration, and spoofing. Users of JH e-mail systems should not assume the confidentiality or integrity of any message that is sent or received via the Internet.

While the transmission and receipt of e-mail messages is generally reliable, timely delivery of time-sensitive information cannot be guaranteed.

Acceptable Use

Acceptable use of e-mail is use that is consistent with the *Use of IT Resources* Policy.

Unacceptable Use

Unacceptable use of Johns Hopkins e-mail systems includes, but is not limited to:

a. Harassing others by sending annoying, abusive, profane, threatening, defamatory, offensive, or unnecessarily repetitive messages.

b. Sending/receiving individually identifiable health information, social security numbers, passwords, or any other Confidential information via the Internet without making reasonable accommodation for the security of such information.

c. Sending e-mail messages from a personal e-mail account that is not owned by the sender without prior approval of the owner.

d. Concealing the identity of the sender, impersonating another, or representing that the sender is someone other than the actual sender.

e. Using JH e-mail to assert or imply that personal views or opinions are the institutional views or opinions of JH.

f. Using JH e-mail systems or address information for any commercial purpose not related to JH.

g. Broadcasting e-mail communications to users or JH e-mail systems without the proper institutional or divisional approval. Such communications are subject to approval by designated JH officials.

h. Intentional distribution of messages that contain viruses, worms, or other malicious code.

3. ANTI-VIRUS POLICY

Electronic viruses, worms, and malicious software are constant threats to the security and safety of computer networks and computing environments. These threats can be minimized by using protected equipment and practice of safe computer habits.

All devices vulnerable to electronic viruses must be appropriately safeguarded against infection and retransmission. Johns Hopkins has licensed anti-virus software for use by faculty, staff, and students. It is the responsibility of every user to ensure that anti-virus protection is current. Infected devices may be blocked and/or removed from the JH Network by IT@JH or appropriate departmental personnel.

Effective (i.e. "endpoint protection") anti-virus protection includes, but is not limited to:

a. Installing anti-virus software on all vulnerable devices

b. Configuring anti-virus software to provide real-time protection

c. Updating anti-virus software with new virus definition files as soon as available

d. Utilizing automated anti-virus updates

e. Executing virus scans on a frequent schedule

f. Refraining from opening e-mail attachments from unknown, suspicious, or untrustworthy sources

g. Refraining from downloading files from unknown or suspicious sources

h. Avoiding direct disk sharing with read/write access unless there is a business requirement to do so

i. Scanning removable media for viruses before use.

Johns Hopkins

Information Technology

Technical and Security Policies

Questions or Comments

A. Introduction

B. Definitions

C. Sponsorship

D. Enforcement

E. Review Cycle

TECHNICAL AND SECURITY POLICIES

1. Disaster Recovery and Business Continuity
2. Electronic Information Classification
3. Network Security
4. Wireless Security
5. Access Control
6. Physical Security of IT Resources
7. Mobile Device/Smart Phone Security
8. Electronic Information Backup, Recovery and Disposal
9. Workstation and Device Security
10. Data Transmission
11. Security Administration of Restricted Systems
12. Vendor
13. Incident Response

1. DISASTER RECOVERY AND BUSINESS CONTINUITY

Disaster Recovery Plans ("DRP") and Business Continuity Plans ("BCP") contain plans and procedures instituted to respond to adverse events that may affect Johns Hopkins in whole or in part. This Policy is concerned with such plans and procedures as they pertain to Johns Hopkins IT Resources and operations. Each JH entity and division is required to develop, maintain, implement, and adhere to plans and procedures for disaster recovery and business continuity according to its own academic and business needs, and consistent with all legal requirements.

These plans include the assessment, notification, and decision processes for declaring a disaster, and, at a minimum, must address the following scenarios:

- Loss of IT personnel
- Loss of local resources
- Loss of the work facility
- Loss of IT connectivity
- Loss of third party IT services

Administrators and managers of IT Resources are responsible for the following functions in their respective areas:

a. Working with the Chief Information Officer or designate to develop appropriate IT DRPs and BCPs, and to prepare funding requests to support DRPs and BCPs.

b. Establishing the procedures necessary to develop, test, and implement DRPs and BCPs, including: obtaining authorization and approval of processes and procedures, securing funding, providing for compliance, performing assessments, activating/de-activating plans, and modifying controls where appropriate.

c. Establishing, funding, and maintaining a set of technology features and operational controls for the entity's IT operations including:

i. Alternate hardware, software, process, and communications resources

ii. Data backup/records retention capabilities

iii. A list of required personnel to support DRP and BCP activities

iv. Necessary support documentation for testing and activation of DRP and BCP.

d. Developing a set of policies, standards, and/or procedures that ensures the effective resumption of critical processes and services in the event of a disruption including:

i. Clinical Operations

ii. Administrative and Financial Operations

iii. Academic and Student Services

iv. Research.

2. ELECTRONIC INFORMATION CLASSIFICATION

Electronic information covered by these Policies falls into one of three classifications below:

1. *Restricted* -- includes *Confidential* and *Internal-use-only*

a. *Confidential*. This includes information required by statutory or common law a high level of protection against unauthorized disclosure, modification, destruction, and use. Confidential information includes, without limitation, the following:

i. Patient medical or billing records and Plan Member records including those covered by the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA)

ii. Student records, including those protected under the Family Educational Rights and Privacy Act (FERPA)

iii. Financial information, including that covered under the Gramm-Leach-Bliley Act (GLBA) and credit card numbers

iv. Employment records, including pay, benefits, personnel evaluations and other staff records

v. Research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq)

vi. Social Security Numbers.

vii. Credit card numbers may not be stored on the JH Network without prior authorization from the institutional treasurer's office and the Chief Information Security Officer.

b. *Internal-use-only*. This includes information that requires protection against unauthorized use, disclosure, modification and/or destruction. Internal-use-only information includes, without limitation, the following:

i. Certain sensitive research data, including information related to a forthcoming or pending patent application

ii. Sensitive information related to Johns Hopkins operations, finances, legal matters, audits, or other business or academic activities

iii. Sensitive information related to donors and potential donors

iv. Information security data, including passwords and information about security-related incidents occurring at Johns Hopkins

v. Internal memos, correspondence, and other documents or information whose distribution is limited as intended by the author and/or administrator.

2. *Unrestricted*. This classification covers information that can be disclosed to any person inside or outside Johns Hopkins. Although security mechanisms are not needed to control disclosure and dissemination, they may still be required to protect against unauthorized modification and destruction of information.

Not all IT Resources require the same level of security or protection mechanisms. Even within the categories of Restricted and Unrestricted information, appropriate security can vary. Security controls must be commensurate with the sensitivity and value of the information resources and actual threats to those resources. Members of the Johns Hopkins community should exercise discretion and judgment when determining how to protect information for which they have responsibility, subject to legal or other obligations of Johns Hopkins. Standards and practices are meant to be flexible enough to change with circumstances.

3. NETWORK SECURITY

It is Johns Hopkins policy to use appropriate tools and practices to protect the Johns Hopkins Network against intrusion and misuse. Network security requires the cooperation of the entire Johns Hopkins community. In order to ensure an effective security monitoring program, installation or use of Security Devices must be in consultation and coordination with the Chief Information Security Officer.

Misuse of the JH Network includes but is not limited to the following:

a. Using the JH Network in violation of any federal, state, or local law

b. Attempting to access portions of the JH Network without authorization

c. Intentionally distributing viruses, worms, or other malicious code using the JH Network

d. Overloading or interfering with the normal functioning of the JH Network or any other network

e. Using any JH managed Internet Protocol ("IP") address without authorization

f. Installing, activating, or configuring any network routing or other device that implements routing protocols (excluding, for example, non-routing switches, hubs, etc.) or a Security Device without prior authorization of the Chief Information Security Officer.

g. Performing scanning, "packet sniffing," eavesdropping, or other forms of data interception on the JH Network without prior authorization of the Chief Information Security Officer.

All JH e-mail systems must utilize security-enabled gateways. IT@JH maintains central gateways that are to be used by all systems. Any exception must be approved by the Chief Networking Officer.

4. WIRELESS SECURITY

Wireless technology presents a number of unique security challenges. For example, it is often difficult for a system or network to know the identity of a user establishing a wireless connection. Wireless security issues are exacerbated by the ease and low cost of deploying wireless access points. Accordingly, the Chief Networking Officer has the responsibility to approve (or designate approval authority to appropriate entities or individuals) wireless network installations. Wireless policies are as follows:

a. Installation of new access points requires registration and coordination with IT@JH and managers of other potentially affected access points.

b. The Chief Networking Officer (or designated approval authority) may disallow the registration and operation of an access point if the access point would result in a conflict with another serving the same area.

c. Authorized access points may shutdown or reconfiguration at a later date, if another academic or administrative unit in the area experiences interference in the relevant frequency ranges.

d. Unencrypted wireless communications are insecure and should not be utilized and are prohibited for Restricted information.

e. Unauthorized interception of wireless communications is considered unacceptable use.

5. ACCESS CONTROL

Only authorized users should have physical, electronic or other access to IT Resources. It is the shared responsibility of administrators and users to prevent unauthorized access to systems at Johns Hopkins. Access controls for IT Resources include (1) effective procedures for granting authorization, (2) tools and practices to authenticate authorized users, and (3) prevention and detection of unauthorized use. Administrators and managers are primarily responsible for establishing, documenting and managing access control policies and processes for their IT Resources.

Authorization

Authorization of access to IT Resources must be based on appropriate business uses (see Use of IT Resources Policy above). Access privileges must be reviewed and revised as appropriate to asset or system risk. If there are changes in job function, student status, transfers, referral privileges and/or JH-affiliation, user authorization should be reviewed and revised. Authorization to access Restricted information must be based on a "need to know" analysis conducted by appropriate systems management, and must be reviewed regularly. As part of a system risk plan, there must be procedures for granting, logging and monitoring emergency temporary user access to Restricted information.

Authentication

IT Resources must have effective authentication tools and practices appropriate to asset or system risk. Systems that provide access to Restricted information must deploy technologies that enforce strong authentication (e.g. strong passwords, bio-metrics, tokens).

Passwords. The following are required password policies for all users:

a. Passwords, especially secure passwords, are often difficult to remember. When users must remember a large number of passwords, they often use insecure methods (e.g. sharing, repeating the same password for each change, posting near the machine) in order to recall passwords. Therefore anyone deploying a new Restricted system should consider password usability for users. This may include providing users with guidance on storing multiple passwords with common utilities (e.g. PasswordSafe).

b. Passwords may not be disclosed intentionally (e.g. disclosed over the telephone) or unintentionally (e.g. written down near the access point or maintained in an accessible electronic file or displayed during key entry). For occasional maintenance or trouble-shooting, it may be necessary for a user to disclose a password to a system administrator. In such cases, it is the user's responsibility to disclose passwords only in person to the administrator (i.e. not by phone or e-mail) and change passwords as soon as practical

Additional Requirements for Systems with Restricted Information. The following are required policies with respect to mission critical systems and those that store, process or transmit Restricted information. In addition, these are recommended best practices for any system:

c. Unique User IDs

d. Creation or issuance of hard-to-guess (strong) passwords, that contain a combination of letters, numbers and special characters and are at least eight (8) characters in length

e. Lock user accounts after five to ten (5 - 10) unsuccessful login attempts

f. Forced periodic password changes (a period of 90 to 180 days is typical)

g. Restrictions on password re-use

h. Banners -- Banners advising users that systems are to be used in compliance with applicable laws, JH policies, that access may be monitored and that privacy and security should be respected by users. Such banners should also state that improper use may result in disciplinary actions.

i. Emergency access for host/system/application administrators -- as part of a system's risk plan, system owners and/or administrators must establish a procedure for emergency, temporary administrative access to IT Resources, even in cases where the primary administrator is unavailable. Such procedures should at a minimum address logging, event triggers, notification and access termination processes.

j. Enterprise credentials -- The confidentiality of enterprise access credentials (e.g. JHED user name and password) is critical, in part, because these credentials often authenticate to multiple Restricted Systems. Server applications that use enterprise credentials for authentication should not collect or cache those credentials. Even making credentials accessible to a server application poses some risk.

Prevention and Detection of Unauthorized Access

Users are to use only their own individual access authorization and not access IT Resources through another user's account.

IT Resources that handle Restricted information must maintain and review access logs. Such access logs should be used to (i) identify questionable data access; (ii) investigate possible breaches; (iii) respond to potential weaknesses (e.g. in coding and systems architecture); and (iv) assess effectiveness of implemented security controls. Audit logging should be deployed in layers: at the network, application and back-end database level and incorporate the following:

- Access logs – host and applications administrators must have a procedure in place to log and review administrative and user access to Restricted systems. For PHI and other Confidential information, record-level access logs must be deployed on Restricted systems.

- Activity logs – it is recommended that user activity (e.g. data insertions, revisions or deletions) be logged and reviewed for high risk data elements or systems.

- System monitoring – the frequency and scope of access monitoring should be appropriate to the system's level of risk. It should be coordinated with other monitoring tools and practices including, for example, monitoring of systems performance, network traffic, and intrusion detection.

6. PHYSICAL SECURITY OF IT RESOURCES

IT Resources must be physically protected commensurate with the level of risk. Systems administrators and managers must ensure that controls are planned and implemented for safeguarding physical components against compromise and environmental hazards. Locks, cameras, alarms and other safeguards as appropriate must be installed in data centers and technology closets to discourage and respond to unauthorized access to electronic or physical components contained in these areas.

- Data centers that store, process and/or transmit Restricted information must have physical access controls commensurate with the level of risk and must include all of the following: (1) card-swipe entry, (2) access logs, (3) access alarms (e.g. to check for propped doors), and (4) guards or video surveillance at all points of entry.

- Facilities with network equipment or a limited number of Restricted servers that must have physical access controls commensurate with the level of risk and must include all of the following: (1) card-swipe entry, (2) access logs, (3) access alarms (e.g. to check for propped doors). It is recommended that guards, video surveillance and hardware monitoring tool be used also.

- Servers that store, process, and/or transmit Unrestricted information exclusively must have physical access controls commensurate with the level of risk and that prevent unauthorized modification and/or destruction.

- To protect against environmental hazards to any system, power, temperature, water and fire monitoring devices are to be deployed as appropriate.

- See the Data Center and Computing Facilities Standards

Users must provide physical security for their IT devices and storage media. Particular care must be paid to securing portable equipment and media -- such as notebook computers, PDAs, tapes, CD's and cellular phones -- especially when traveling in order to protect these devices. Confidential information may not be stored on portable devices or other media unless encrypted.

Device Encryption -- It is the responsibility of system administrators to assess risk regarding physical loss or theft of mobile and stationary devices. Appropriate security controls to address these risks include physical security safeguards above, restrictions on access and encryption.

- All laptops and mobile devices reasonably likely to be used to store Restricted information must have full disc encryption installed and activated. Laptop computers and mobile devices used by Johns Hopkins Medicine personnel for work purposes (including peronally owned devices) are presumed to be reasonably likely to store Restricted information unless designated otherwise by appropriate staff.

- All at-risk workstations (e.g. JHM clinical, accessible to the public, open spaces, etc.) reasonably likely to store Restricted information must have full disc encryption installed and activated.

- All servers storing Restricted information (e.g. file servers, email servers, databases) must be stored in a data center or otherwise secure area as described above. It is strongly recommended that such servers be placed in full service data centers.

7. MOBILE DEVICE/SMART PHONE SECURITY

Policy 6 above addresses physical security of mobile devices, including the statement, "Confidential information may not be stored on portable devices or other media unless encrypted." Security for handheld devices, many of which serve as telephones and text message communicators, has several unique characteristics:

a. Use enterprise-supported devices where possible so as to ensure appropriate security settings.

b. When performing initial setup or maintenance on the device, be sure to access Hopkins messaging directly (e.g. through ActiveSync on Exchange) and minimize the chance that messages or user credentials will be sent in clear text. Also avoid disclosing JH credentials to vendors and support staff.

c. Choose a strong password or PIN. The security of your system is only as strong as the password. It may be difficult to type especially complex passwords on the small keypad of some devices, but it is important to create the strongest reasonable passwords.

d. Minimize data exposure by limiting the number of messages stored on the mobile device. In some cases, this requires users or administrators to change default device settings.

e. Email and address books, while not Restricted information, should be considered sensitive and worth protection.

f. Keep current with OS and security updates. As threats emerge, it may become necessary to install additional security, including anti-virus, anti-spyware and/or intrusion detection.

g. Verify encryption mechanisms for data at rest (where Restricted information is likely to be stored) and transmissions. Accounts and/or passwords may not be transmitted over wireless networks. Johns Hopkins Secure Connect VPN provides encryption for many device types.

h. Use remote "kill" functionality where possible. These allow users or administrators to delete data from a lost or stolen device rapidly.

i. Promptly report lost or stolen devices.

j. Reduce security risk by limiting your device to only necessary applications and services. Unnecessary applications may create security and usability issues and drain device bandwidth and battery life. Bluetooth and IR are two examples of services that can open devices to unwelcome access if improperly configured.

k. Follow- safe disposal practices by removing all sensitive information first. Enterprise-supported devices will generally back this up.

8. ELECTRONIC INFORMATION BACKUP, RECOVERY AND DISPOSAL

Backup, recovery and disposal procedures are required for business-critical systems at Johns Hopkins, and recommended for any system.

Back-up and Recovery. System administrators and managers of business critical systems or those related to Restricted information must have documented procedures to create a retrievable, exact copy of critical information and must test data and systems recovery regularly. Requirements for back-up and recovery include the following:

a. Restricted information must be regularly backed-up on durable media using documented handling procedures that should include a provision for off-site storage.

b. Restricted information stored on an external medium must be protected from theft and unauthorized access including provision of security when external media or under the control of a third party (e.g. courier, off-site

back-up).

c. Restricted information stored on an external medium must be labeled appropriately and the label should include the creation date.

d. Portable back-up media that may contain Restricted information must be encrypted. It is the responsibility of administrators to assess the risk and practicality of encrypting media that is currently in archival form whether on-site or located at a third party facility.

In addition to these standards, certain Restricted information may include specific legal requirements for systems back-up and recovery. Unrestricted information are to be backed up as appropriate to the level of risk for loss of information and/or its impact on systems and interfaces.

Disposal. Restricted information must be disposed of in such manner as to ensure it cannot be retrieved or recovered. When donating, selling, transferring, or disposing of computers or removable media, care must be taken to ensure that Restricted data is rendered unreadable by, for example, defacement, degaussing or other standard techniques. It is insufficient to simply "delete" information (or reformat) from most storage media as that information is often easily recovered.

9. COMPUTING DEVICE SECURITY

Administrators, managers and users share the responsibility of maintaining the security of servers, workstations and other computing devices.

Administrators and users managing their own devices are required to:

a. Protect any device under their management from compromise.

b. Modify default installation passwords and other configuration options to reduce vulnerabilities to a minimum.

c. Install updated anti-virus (see *Anti-Virus Policy* above) relevant security patches to fix security issues

d. Periodically verify audit and activity logs, examine performance data, and generally check for any evidence of unauthorized access, the presence of viruses or other malicious code.

e. Cooperate with IT@JH by providing support for and/or review of administrative activities as well as performing more sophisticated procedures such as penetration testing and real-time intrusion detection.

Administrators and managers who develop, maintain, or modify critical applications relating to Restricted information must deploy adequate procedures for change control, separation of test and production environments, and separation of responsibilities for staff involved in these functions. They must actively cooperate with IT@JH, the Office of Hopkins Internal Audits and other JH administrative entities working in application security.

10. DATA TRANSMISSION

Despite efforts to secure it, traffic on the JH Network could be surreptitiously monitored by unauthorized parties. While the risk of such compromise is considerably greater for transmissions across the Internet, JH Network perimeter controls cannot provide complete security. It is therefore the responsibility of administrators and users to avoid using insecure transmission protocols -- such as e-mail, Instant Messaging, rlogin, ftp and telnet -- that may transmit unencrypted authentication credentials (e.g. passwords) or Restricted payloads:

a. External Transmissions of Restricted Information

(i) *Any transmission* -- Restricted information should not be transmitted across public networks (i.e. the Internet) in clear text. Encryption and password protection of attachments are generally reasonable protections for transmission of such information to external entities and should be deployed as appropriate for Restricted information in, for example, e-mail and instant messaging (IM).

(ii) Transmissions of large files -- Except with prior authorization of the Chief Information Security Officer, it is prohibited to transmit across public networks in clear text:

- Substantial amounts, or otherwise high risk, Restricted information; such transmissions should also authenticate recipients and validate that transmissions have occurred.

- Authentication credentials to JH systems (in particular administrative access passwords). Even a single administrative password transmitted insecurely (e.g. outbound send, incoming remote log-in) could pose a substantial risk.

- It is prohibited for users likely to send or receive Restricted information (e.g. JHM personnel, HR professionals) through email to forward JH email accounts to third party web email services (e.g. Yahoo, Hotmail, Gmail).

b. Internal Transmissions of Restricted Information

(i) New applications and/or interfaces involving Restricted information must, where possible, be capable of securing transmissions. New applications and/or interfaces should thus secure transmissions of Restricted information (both credentials and payloads)

(ii) It is the responsibility of administrators of existing applications and/or interfaces to formally assess the practicality of migrating insecure transmissions to secure alternatives and to periodically update this assessment as new technologies are made available

(iii) Deploying point-to-point communications or transmitting behind internal application firewalls are generally deemed reasonable security controls. Administrators may choose to supplement such controls with encryption as appropriate.

11. SECURITY ADMINISTRATION OF RESTRICTED SYSTEMS

Systems or applications that store, process or transmit Restricted information require more intensive security at technical and managerial levels. Preserving the confidentiality, integrity and availability of sensitive information and business-critical systems requires managerial leadership, conscientious users and sound technical practice.

As the purpose and functions of systems vary, administrators (including, without limitation, those for networks, hosts, applications, devices, databases and interfaces) should refer to specific JH Standards for guidance and industry best practices. This policy outlines high level guidance:

a. Systems Documentation – Restricted systems should have documentation regarding asset management, configuration, maintenance, security, disaster recovery and compliance. An inventory of equipment storing Restricted information must be maintained. Inventory procedures should include provision for equipment disposal or movement of equipment off-site and between JH campuses, including responsible parties and major repairs or configuration changes.

b. Risk Assessment – Administrators of Restricted systems should conduct or solicit periodic (at least every three years) risk assessments regarding administrative, physical and technical vulnerabilities. Risk assessments should include inventories of interfaces, connectivity, vendor documentation and testing where appropriate. Risk assessments should be conducted in consultation with (internal or external) experts on security risk and in

cooperation with technical and operational management. Documentation should include enumeration of security gaps and updated remediation plans. In addition, administrators should work with operational management to determine whether use of private Restricted information is the minimum necessary to accomplish business objectives. Please see current JH Risk Assessment Guidance for instructions.

c. Disabling Unnecessary Services – Restricted systems must have services disabled that are not required to achieve the business purpose of the system (e.g. FTP, Telnet, SMTP, etc).

d. Virus Protection – Restricted systems must maintain automated virus detection update mechanisms. Updates should be automatic and transparent where practical, otherwise automatic reminders are required. It is also recommended that controls be implemented to protect against other malicious code as threats evolve (e.g. spyware).

e. Patch Management – Restricted systems must have controls in place to provide timely notification regarding relevant patches. Administrators have the responsibility to determine whether and/or when to deploy patches. In cases where IT@JH recommends deployment of a patch, administrators must deploy patches in a timely fashion or otherwise implement and document compensating controls.

f. Intrusion Detection and Monitoring – Johns Hopkins has deployed network intrusion detection (NIDS). NIDS is generally more effective when combined with host-based or application-level intrusion detection or monitoring. It is therefore recommended that administrators deploy these tools to supplement perimeter controls. Such may include, for example, automated access logging, integrity checking, or signature-based intrusion detection.

g. Administration -- administration of Restricted systems may only be performed by authorized, trained personnel. Remote administration of Restricted systems requires strong authentication, stringent authorization, transmission encryption, and regular review of administrator and user access logs.

h. Data Security -- Restricted information should be physically separated from application or system services (e.g. application middleware, Web and e-mail servers, etc).

i. Vulnerability Scanning – there should be routine monitoring and remediation of equipment for vulnerabilities, specifically regarding components connected to the JH Network.

j. Web servers -- Web-sites and Web applications should be documented and reviewed routinely for Web-based vulnerabilities and the possibility of unauthorized access to Restricted information on the Web-site or on the server.

k. Automatic Log-off -- systems, applications and/or devices used routinely to access Restricted information must terminate/lock/suspend electronic sessions after a reasonable period of inactivity. Appropriate idle time depends upon the use, location and type of system and information.

l. Equipment Placement -- Equipment should be positioned and configured so as to minimize the likelihood of unauthorized individuals intentionally or inadvertently viewing or otherwise accessing Restricted information. Appropriate risk assessments document opportunities for "shoulder surfing" regarding devices in public areas, including, without limitation, walkways, waiting areas, libraries and examination rooms.

m. Training and Awareness – technical and operational management should coordinate electronic system access with training that includes security awareness. Technical staff should include security as part of on-going skills development.

12. VENDOR

Vendors play an important role in providing and often supporting information technology solutions at Johns Hopkins. The standard of care concerning the use, support and administration of IT Resources is no less

stringent than it is for JH personnel.

a. Johns Hopkins will provide a point of contact for the vendor. This contact person will work with the vendor and other relevant Johns Hopkins personnel (for example, legal counsel, business and IT management) to ensure compliance with JH policies.

b. Vendors must comply with all applicable policies, requirements, standards and agreements, including, those established at an institutional and/or JH entity level (e.g. requirements for effective anti-virus protection).

c. Vendors are required to cooperate with JH personnel on testing security, reliability, inter-operability, usability and other potential impacts on IT and operational environments at Johns Hopkins.

d. Vendors are obligated to notify appropriate JH personnel promptly of any defects or incidents that might be material to the on-going operation or security of IT Resources at JH.

e. Vendors are required to work with appropriate JH personnel to establish procedures for creating, modifying or eliminating services or configurations. Such procedures must be documented and include mechanisms for testing modifications and notifying affected JH stakeholders.

Vendor Access

As part of their support function, vendors may be granted access, rights and privileges with respect to JH IT Resources normally afforded only to JH personnel. Because third-party access poses risk, access must be strictly controlled, particularly when it involves Restricted information or critical IT Resources.

a. Vendor access to IT Resources is conferred to specific identifiable persons. Access must be limited to specific resources, tasks and functions only for the time period required to accomplish approved tasks. There must be procedures for terminating individual access upon completion of or removal from approved tasks.

b. Vendors are required to comply with laws and JH policies regarding the confidentiality of Restricted information to which they have access. They must take all reasonable steps, based upon applicable industry standards to protect JH IT Resources from corruption, tampering, or other damage.

c. Third party hosting of Restricted applications requires contract review by a JH counsel's office. It is often the case that standard terms and conditions from hosting sites do not provide adequate assurances regarding privacy and security.

d. Johns Hopkins is responsible for issuing unique individual accounts. Under exceptional circumstances, responsibility for issuing individual accounts may be delegated to vendors.

e. It is prohibited to share accounts even if individuals share certain administrative or support responsibilities.

f. Upon request the vendor must be prepared to do the following:

(i) Identify IT Resource(s) and information to which the vendor will be granted access

(ii) Identify the business purpose for which access is to be granted and limitation of access to that purpose

(iii) Provide access logs that capture individual identity and timing and duration of access and be maintained for no less than 90 days

(iv) Provide descriptions of security policies and practices.

g. All vendor personnel, physically accessing a JH facility must be able to provide adequate identification.

h. Vendor access to JH IT resources may be re-certified annually.

i. Violations of this policy may result in the loss of vendor access to JH IT Resources and/or other legal or contractual recourse.

13. INCIDENT RESPONSE (incident@jhu.edu)

Johns Hopkins will take steps to remediate, respond to and recover from security incidents related to JH IT Resources. Depending on the nature of the incident, this may involve but not be limited to the following:

- collecting and analyzing evidence
- determining responsible parties
- assessing damages
- restoring data from backup files
- correcting security vulnerabilities
- implementing appropriate security controls
- revising security guidelines and procedures
- taking disciplinary action in accordance with appropriate JH policies
- reporting incidents to appropriate authorities

The JH Computer Incident Response Team (JH-CIRT) has the responsibility to investigate security incidents and coordinate response and recovery.

Covered Personnel are required to report suspected or known security incident(s) of IT Resources to appropriate divisional or organizational management and/or to others as outlined below.

a. *Technical Reporting* – Covered Personnel should report incidents such as virus attacks or other computer-related disruptions to appropriate technical staff (e.g. server or workstation support, application support, help desk, department manager). It is the responsibility of technically knowledgeable staff to evaluate user reports and relay appropriate information to the JH-CIRT. Incidents that have the potential to damage departmental and/or JH network operations should be reported immediately.

b. *Physical Security Reporting* -- Incidents that principally involve theft, destruction, and/or other illegal activity related to IT Resources should be reported to the appropriate building, campus or corporate security departments. Security departments coordinate with the JH-CIRT to investigate and evaluate potential compromises of networks and sensitive information.