

Chief Information  
Officer

Strategic  
Framework

Featured  
Projects

News & Alerts

Search

Clear



Home

Getting Started

Connectivity

Email

Support

Site Tools

[Print This Page](#)

#### Administrative Applications

- Select A Link -

#### Clinical Applications

- Select A Link -

#### Enterprise Services

- Select A Link -

#### Student Services

- Select A Link -

#### Support

- Select A Link -

#### Teaching & Learning

- Select A Link -

#### Technical Professionals

Contact IT@JH

A. [Introduction](#)

B. [Definitions](#)

C. [Sponsorship](#)

D. [Enforcement](#)

E. [Review Cycle](#)

### USE POLICIES

1. [Use of IT Resources Policy](#)

2. [E-mail Use Policy](#)

3. [Anti-virus Policy](#)

#### 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 expanded dramatically over the last twenty years, and it is likely that the rate of change will accelerate. 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 these resources are 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 users
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. Neither this policy nor present technology is able to guarantee security, privacy or confidentiality. It is the routine policy of JH IT administrators to view or disclose the content of others' e-mail. Johns Hopkins reserves the right, and may be legally required, to access, copy, examine, and/or disseminate any e-mail or transmitted on, across or through JH IT Resources, in a number of circumstances.

## Johns Hopkins Information Technology Use Policies [Questions or Comments](#)

security, and/or legal purposes; as needed to maintain or protect its personnel, facility status; as necessary to maintain network services; or in order to protect JH's rights. 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 of students or staff; and other information protected by the attorney-client privilege) is shared with persons with access to such information are expected to be aware of and comply fully with policies protecting such information. Nothing in these Policies is intended to affect in any way the creation or protection of such information.

Johns Hopkins complies fully with all federal, state, and local laws, including the Digital Millennium Copyright Act. All legal questions should be directed to the JHU Office of General Counsel or the General Counsel for the respective entity, school, or department involved.

The *Use Policies* were approved by the ICSC, Chief Information Officer and Council in November 2005. The *Technical and Security Policies* were approved by the ICSC, Chief Information Officer in September, 2005 and revisions approved in November 2006 and April 2007.

## **B. DEFINITIONS**

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

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

*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; handhelds; printers; software; data on other storage media; hubs, routers, cables; and all other internal and external communications resources. IT Resources acquired by Johns Hopkins are considered

*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 entities of 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, and wireless access points.

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

*Security Device* – IT Resources that provide for the confidentiality, integrity and availability of information resources connected to the JH Network. Examples of Security Devices include vulnerable 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 independence, and each such entity or division is encouraged to develop, maintain, and improve its own procedures and practices, including authorization procedures, to implement these Policies for its own academic or business needs.

## **D. ENFORCEMENT**

The failure by Covered Personnel to comply with these Policies may result in loss of

of IT Resources and/or loss of access privileges to IT Resources. In addition, violator may be subject to criminal and/or civil penalties and to disciplinary action, up to and

## **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' mission: research, service, and patient care, and is legal, ethical, and honest. Acceptable use includes intellectual property, ownership of data, system security mechanisms, and individual rights and freedom from intimidation, harassment, and annoyance. Further, it must show responsible consumption and utilization of IT Resources, and it must not jeopardize Johns Hopkins' status. Incidental personal use of IT Resources is permitted if consistent with applicable policy, and if such use is reasonable, not excessive, and does not impair work performance.

#### **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, or unnecessarily repetitive messages, or by sending e-mails that appear to come from the sender
- d. Any activity designed to hinder another person's or institution's use of its own information 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 "sniffing" software, offensive applications, and malicious software).
- g. Any use of copyrighted materials in violation of copyright laws or of vendor licenses (e.g., illegal downloading and/or sharing of media files or computer software)
- h. Intentional, non-incidentally acquired, storage, and/or display of sexually explicit material for non-acknowledged, legitimate medical, scholarly, educational, or forensic purposes. Exposure of such material may be offensive, constitute sexual harassment or create a hostile work environment.
- i. Security breaches, intentional or otherwise, including improper disclosure of a password or 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, without specific authorization, to imply JH support (as opposed to personal position or proposition)
- l. Use to engage in activities, including for example certain political activities, prohibited by 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 and sophistication. Policies and procedures regarding e-mail storage, back-up, and access are consistent across JH. In addition, there is no single e-mail archive system for the

Back-up, storage and archiving of important e-mail messages are the responsibility of the user.

E-mail transmission over the Internet is inherently insecure and subject to security breaches, message interception, message alteration, and spoofing. Users of the JH e-mail system 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, or unnecessarily repetitive messages
- b. Sending/receiving individually identifiable health information, social security numbers, or any other Confidential Information via the Internet without making reasonable accommodations for the security of such information
- c. Sending e-mail messages from a personal e-mail account that is not owned by the user without prior approval of the owner
- d. Concealing the identity of the sender, impersonating another, or representing oneself as someone other than the actual sender
- e. Using JH e-mail to assert or imply that personal views or opinions are the institutional opinions of JH
- f. Using JH e-mail systems or address information for any commercial purpose not approved by the user's department
- g. Broadcasting e-mail communications to users of JH e-mail systems without the divisional approval. Such communications are subject to approval by designated JH representatives
- h. Intentional distribution of messages that contain viruses, worms, or other malicious software

## **3. ANTI-VIRUS POLICY**

Electronic viruses, worms, and malicious software are constant threats to the security of computer networks and computing environments. These threats can be minimized through the use of anti-virus equipment and practice of safe computer habits.

All devices vulnerable to electronic viruses must be appropriately safeguarded against 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 files may be blocked and/or removed from the [JH Network](#) by IT@JH or appropriate departmental representatives.

Effective 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 untrusted 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 re
- 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. [Electronic Information Backup, Recovery and Disposal](#)
8. [Workstation and Device Security](#)
9. [Data Transmission](#)
10. [Security Administration of Restricted Systems](#)
11. [Vendor](#)
12. [Incident Response](#)

**1. DISASTER RECOVERY AND BUSINESS CONTINUITY**

Disaster Recovery Plans (“DRP”) and Business Continuity Plans (“BCP”) contain plan instituted to respond to adverse events that may affect Johns Hopkins in whole or in concerned with such plans and procedures as they pertain to Johns Hopkins [IT Reso](#) Each JH entity and division is required to develop, maintain, implement, and adhere procedures for disaster recovery and business continuity according to its own acadei needs, and consistent with all legal requirements.

These plans include the assessment, notification, and decision processes for declarir 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 functional areas:

- a. Working with the Chief Information Officer or designate to develop appropriate IT to prepare funding requests to support DRPs and BCPs.
- b. Establishing the procedures necessary to develop, test, and implement DRPs and obtaining authorization and approval of processes and procedures, securing funding compliance, performing assessments, activating/de-activating plans, and modifying appropriate.
- c. Establishing, funding, and maintaining a set of technology features and operational 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 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

1. *Restricted* -- includes *Confidential* and *Internal-use-only*
  - a. *Confidential*. This includes information required by statutory or common law a h against unauthorized disclosure, modification, destruction, and use. Confidential information 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, credit card numbers
    - iv. Employment records, including pay, benefits, personnel evaluations and other
    - v. Research data involving human subjects that are subject to the Common Rule 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 approval from the institutional treasurer's office and the Chief Information Security Officer.
  - b. *Internal-use-only*. This includes information that requires protection against unauthorized

disclosure, modification and/or destruction. Internal-use-only information includes, the following:

- i. Certain sensitive research data, including information related to a forthcoming patent application
- ii. Sensitive information related to Johns Hopkins operations, finances, legal matters 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 incidents occurring at Johns Hopkins
- v. Internal memos, correspondence, and other documents or information whose use is limited as intended by the author and/or administrator.

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

Not all IT Resources require the same level of security or protection mechanisms. Even within categories of Restricted and Unrestricted information, appropriate security can vary. Security must be commensurate with the sensitivity and value of the information resources and those resources. Members of the Johns Hopkins community should exercise discretion in determining how to protect information for which they have responsibility, subject to the obligations of Johns Hopkins. Standards and practices are meant to be flexible enough to accommodate changing 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 of 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 portion thereof
- e. Using any JH managed Internet Protocol ("IP") address without authorization
- f. Installing, activating, or configuring any network routing or other device that implements network protocols (excluding, for example, non-routing switches, hubs, etc.) or a Security Device without the 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 a policy that must 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, a system or network to know the identity of a user establishing a wireless connection. These issues are exacerbated by the ease and low cost of deploying wireless access points. The Chief Networking Officer has the responsibility to approve (or designate approval authority for)

entities or individuals) wireless network installations. Wireless policies are as follow

- a. Installation of new access points requires registration and coordination with IT@JHU and other potentially affected access points.
- b. The Chief Networking Officer (or designated approval authority) may disallow the operation of an access point if the access point would result in a conflict with another area.
- c. Authorized access points may need to be shut down or reconfigured at a later date if an administrative unit in the area experiences interference in the relevant frequency.
- d. Unencrypted wireless communications are insecure and should not be utilized to transmit Restricted information.
- e. Unauthorized interception of wireless communications is considered unacceptable.

## 5. ACCESS CONTROL

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

### Authorization

Authorization of access to IT Resources must be based on appropriate business uses (see Resources Policy above). Access privileges must be reviewed and revised as appropriate to system risk. If there are changes in job function, student status, transfers, referral to another JHU-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 staff and must be reviewed regularly.

### Authentication

IT Resources must have effective authentication tools and practices appropriate to a system. Systems that provide access to Restricted information must deploy technologies that support 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 using 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. When deploying a new Restricted system should consider password usability for users. This includes providing users with guidance on storing multiple passwords with common utilities (e.g. password managers).
- b. Passwords may not be disclosed intentionally (e.g. disclosed over the telephone) or written down near the access point or maintained in an accessible electronic file or cloud storage (e.g. email). For occasional maintenance or trouble-shooting, it may be necessary for a user to provide a password to a system administrator. In such cases, it is the user's responsibility to communicate the password 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 additional requirements 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 upper and lower case 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 advising users that systems are to be used in compliance with applicable that access may be monitored and that privacy and security should be respected by should also state that improper use may result in disciplinary actions.

### **Prevention and Detection of Unauthorized Access**

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

IT Resources that handle Restricted information must maintain and review access logs should be used to (i) identify questionable data access; (ii) investigate possible breaches and 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 review administrative and user access to Restricted systems. It is recommended that real-time access logs be deployed where there are high risk data elements (e.g. financial information)
- Activity logs – it is recommended that user activity (e.g. data insertions, revisions, 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 a system's level of risk. It should be coordinated with other monitoring tools and procedures. 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. System administrators and managers must ensure that controls are planned and implemented for safeguarding hardware components against compromise and environmental hazards. Locks, cameras, alarm systems, and other safeguards as appropriate must be installed in data centers and technology closets to detect and respond to unauthorized access to electronic or physical components contained in them.

- Data centers that store, process and/or transmit Restricted information must have physical security controls commensurate with the level of risk and must include all of the following: (1) access control, (2) access logs, (3) access alarms (e.g. to check for propped doors), and surveillance at all points of entry.
- Facilities with network equipment or a limited number of Restricted servers that store, process and/or transmit Restricted information must include all of the following: (1) access control, (2) access logs, (3) access alarms (e.g. to check for propped doors). It is recommended that guards, video surveillance and hardware monitoring be implemented.
- 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 access and destruction.
- To protect against environmental hazards to any system, power, temperature, and humidity 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 attention must be given to securing portable equipment and media -- such as notebook computers, PDAs, tablet PCs, and mobile phones -- especially when traveling in order to protect these devices. Confidential information must not be stored on portable devices or other media unless encrypted.

Device Encryption -- It is the responsibility of system administrators to assess risk related to the loss or theft of mobile and stationary devices. Appropriate security controls to address this risk must be implemented.

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.
- All at-risk workstations (e.g. 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 placed in a data center or otherwise secure area as described above. It is strongly recommended that all servers be placed in full service data centers.

## 7. ELECTRONIC INFORMATION BACKUP, RECOVERY AND DISPOSAL

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

**Back-up and Recovery.** System administrators and managers of business critical systems storing Restricted information must have documented procedures to create a retrievable backup of Restricted information and must test data and systems recovery regularly. Requirements for backup procedures include the following:

- a. Restricted information must be regularly backed-up on durable media using documented 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 is transported (e.g. under the control of a 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 and to determine the archival form whether on-site or located at a third party facility.

In addition to these standards, certain Restricted information may include specific requirements for systems back-up and recovery. Unrestricted information are to be backed up as appropriate based on the 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 recovered. When donating, selling, transferring, or disposing of computers or removable media, appropriate steps must be taken to ensure that Restricted data is rendered unreadable by, for example, defragmentation or other standard techniques. It is insufficient to simply "delete" information (or remove it from storage media as that information is often easily recovered).

## 8. COMPUTING DEVICE SECURITY

Administrators, managers and users share the responsibility of maintaining the security of 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 vulnerability to a minimum
- c. Install updated anti-virus (see [Anti-Virus Policy](#) above) relevant security patches
- d. Periodically verify audit and activity logs, examine performance data, and generate reports. 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 actions and by performing more sophisticated procedures such as penetration testing and real-time monitoring.

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

## 9. DATA TRANSMISSION

Despite efforts to secure it, traffic on the JH Network could be surreptitiously monitored by parties. While the risk of such compromise is considerably greater for transmissions across the 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, Messaging, rlogin, ftp and telnet -- that may transmit unencrypted authentication credentials (such as passwords) or Restricted information payloads:

### a. External Transmissions of Restricted Information

(i) *Any transmission* -- Restricted information should not be transmitted across the Internet in clear text. Encryption and password protection of attachments are reasonable protections for transmission of such information to external entities; such protections 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 be encrypted and authenticate recipients and validate that transmissions have occurred
- Authentication credentials to JH systems (in particular administrative access passwords) or administrative passwords transmitted insecurely (e.g. outbound send, incoming responses) pose a substantial risk.

### b. Internal Transmissions of Restricted Information

(i) *New applications and/or interfaces* involving Restricted information must be capable of securing transmissions. New applications and/or interfaces should be designed to support secure transmissions of Restricted information (both credentials and payloads)

(ii) *It is the responsibility of administrators of existing applications and/or interfaces* to periodically 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 firewalls* are generally deemed reasonable security controls. Administrators may supplement such controls with encryption as appropriate.

## 10. SECURITY ADMINISTRATION OF RESTRICTED SYSTEMS

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

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

a. *Systems Documentation* -- Restricted systems should have documentation regarding their management, configuration, maintenance, security, disaster recovery and compliance. Documentation for equipment storing Restricted information should be maintained.

b. *Risk Assessment* -- Administrators of Restricted systems should conduct periodic risk assessments.

against current electronic and physical vulnerabilities. Risk assessments should include interfaces, vendor documentation and testing where appropriate. In addition, administrators should work with operational management to determine whether use of private information is the

c. **Disabling Unnecessary Services** – Restricted systems must have services disabled to achieve the business purpose of the system (e.g. FTP, Telnet, SMTP, etc).

d. **Virus Protection** – Restricted systems must maintain automated virus detection and updates. Updates should be automatic and transparent where practical, otherwise manual updates required. It is also recommended that controls be implemented to protect against threats that evolve (e.g. spyware).

e. **Patch Management** – Restricted systems must have controls in place to provide transparency regarding relevant patches. Administrators have the responsibility to determine 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 systems. NIDS is generally more effective when combined with host-based or application-level monitoring. It is therefore recommended that administrators deploy these tools to supplement existing controls. Such may include, for example, automated access logging, integrity checking, and network intrusion detection.

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

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

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

j. **Web servers** -- Any Web-site or application should be documented and reviewed regularly for vulnerabilities and the possibility of unauthorized access to Restricted information on the server.

## **11. VENDOR**

Vendors play an important role in providing and often supporting information technology services at Johns Hopkins. The standard of care concerning the use, support and administration of these services is less stringent than it is for JH personnel.

a. Johns Hopkins will provide a point of contact for the vendor. This contact person should be a member of the vendor and other relevant Johns Hopkins personnel (for example, legal counsel, business 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 data protection).

c. Vendors are required to cooperate with JH personnel on testing security, reliability, performance, 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 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 testing, 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

IT Resources normally afforded only to JH personnel. Because third-party access must be strictly controlled, particularly when it involves Restricted information or critical IT

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

b. Vendors are required to comply with laws and JH policies regarding the confidential information to which they have access. They must take all reasonable steps, based on current industry standards to protect JH IT Resources from corruption, tampering, or other misuse.

c. Third party hosting of Restricted applications requires contract review by a JH controller. It is often the case that standard terms and conditions from hosting sites do not provide adequate protection 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 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 limit access to that purpose
- (iii) Provide access logs that capture individual identity and timing and duration of access, which are 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 a valid photo ID.

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 contractual recourse.

## **12. INCIDENT RESPONSE ([incident@jhu.edu](mailto:incident@jhu.edu))**

Johns Hopkins will take steps to remediate, respond to and recover from security incidents. See [Resources](#). Depending on the nature of the incident, this may involve but not be limited to:

- 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 incidents and coordinate response and recovery.

Covered Personnel are required to report suspected or known security incident(s) of concern 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, computer-related disruptions to appropriate technical staff (e.g. server or workstation).

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 result in damage to departmental and/or JH network operations should be reported immediately.

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

**Questions or Comments**