Acceptable Use and Security of Johns Hopkins Information Technology Resources

Guideline: TECH001
Responsible Executive: Chief Information Security Officer
Responsible Office: IT@JHU Office of CIO
Approved by: Senior Planning Group
Effective: 01/01/2019
Last Revised: N/A

Table of Contents

Policy Statement

The Policies on Acceptable Use and Security of Johns Hopkins Information Technology Resources ("IT Policies") set out requirements, responsibilities, and expectations for all users of Johns Hopkins IT Resources, as defined below. The IT Policies also describe specific security responsibilities for custodians of restricted information and systems administrators.

Who Is Governed By This Policy

All persons with contents in storage on the Johns Hopkins Network ("JH Network") and networks contracted by Johns Hopkins (as noted in the definitions, networks managed by the Applied Physics Laboratory) are subject to the IT Policies and all relevant institutional policies.

Johns Hopkins recognizes that entities and divisions of Johns Hopkins operate 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 IT Policies according to its own academic or operational needs. Each entity or division is also welcome to adopt more restrictive security procedures and practices, in consultation with IT@JH.

Purpose

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, clinical care and other professional practice and services, and plays a central role in the overall life of the institution. It is critical, therefore, that we ensure that our technology is secure, reliable, and available for the entire Johns Hopkins community.

Despite Johns Hopkins' security efforts, internet communications (e.g., e-mail, instant messaging) may not be secure and may be subject to issues such as message interception, message alteration, and spoofing. Accordingly, policies are needed to inform users of Johns Hopkins IT Resources about the risks involved in their use of these resources (e.g., they should not assume the confidentiality or integrity of all internet communications), and to empower users to mitigate those risks where possible.

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

The IT Policies do not replace obligations under applicable federal, state, and local laws; Johns Hopkins complies fully with these 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 research 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.

Definitions

Defines terms in alphabetical order that are used in the policy or related procedures, including technical terms that readers may not understand.

Confidential	See below, Electronic Information Classification.
Covered Personnel	Covered Personnel includes faculty, staff, employees, students, volunteers, officers, trustees, guests, visitors, and other workforce members, such as casual workers, consultants, temporary staff, and vendors. Johns Hopkins does not normally enforce penalties for misconduct off the JH Network or on JH physical premises. However, electronic misconduct directed by Covered Personnel against others in the Hopkins community or elsewhere may be actionable regardless of the location from which the misconduct originated or the network or devices used. Privately-owned computer systems or mobile devices, or those owned by JH organizations or by collaborative research projects, when connected to the JH Network, are subject to the same responsibilities and regulations as pertain to JH-owned devices and systems.
IT Resources	Information technology ("IT") Resources of Johns Hopkins 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.
Internal Use Only	See below, Electronic Information Classification.
Johns Hopkins and JH	These terms 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; All-Children's General Hospital, Suburban Hospital, Sibley Memorial Hospital, Johns Hopkins Community Physicians; and all of the clinics, schools, divisions, departments, and affiliated corporations of any or all of these entities.

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. The JH Network does not include networks managed by the JHU Applied Physics Laboratory. Examples of network resources are hubs, routers, cables, switches, wireless access points and Security Devices.
Restricted	see below, Electronic Information Classification Policy.
Security Device	IT Resources that provide for confidentiality, integrity and availability of IT resources connected to the JH Network. Examples of Security Devices include, without limitation, vulnerability scanners, network firewalls, password crackers, penetration tools and network/server intrusion detection monitors and sensors. General purpose IT tools or programs fall under this definition insofar as they are used for similar purposes.
Sensitive	see below, Electronic Information Classification Policy.
Unrestricted	see below, Electronic Information Classification Policy.

Policy Set

I. **Acceptable Use Policy**

A. ***Acceptable Use***

Acceptable use of Johns Hopkins 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, institutional reputation and an individuals' rights to privacy and freedom from harassment and discrimination. Further, it must show consideration in the consumption and utilization of IT Resources, and it must not jeopardize Johns Hopkins' not-for-profit status. As representatives of the JH community, Covered Personnel are expected to consider the institution's reputation when engaged in electronic dealings with those both within and outside JH.

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.

B. ***Unacceptable Use***

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

1. **In General**
   a. Use of IT Resources in violation of any Johns Hopkins policies and/or applicable law;
   b. Any activity that hinders Johns Hopkins, its Covered Personnel, or another person's or institution's use of its information technology resources;
   c. Any use of copyrighted materials in violation of applicable intellectual property laws or of vendor licensing agreements (e.g., illegal downloading and/or sharing of media files or computer software);
   d. Use to engage in activities, including for example certain political activities, prohibited to tax exempt 501 (c) (3) organizations;
   e. Commercial use of IT Resources for business purposes not related to Johns Hopkins;

f. Stand-alone or remotely-controlled cameras and other recording devices used in places or ways that violate a reasonable expectation of privacy on the part of those whose activities are intentionally or incidentally recorded;

2. **Access, Authorization and Security**
   a. Unauthorized access to or unauthorized use of IT Resources;
   b. Use of mobile IT Resources (laptops, portable devices) storing Restricted information without encryption;
   c. Intentional or careless distribution of viruses, worms, or other malicious code;
   d. Installation of inappropriate software or hardware on IT Resources (e.g., network or password "sniffing" software, penetration tools, and malicious software);
   e. 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;
   f. Unauthorized disposal of IT Resources;
   g. Failure to follow the security requirements described below in "General User Security";
3. **Communications**
   a. Sending or posting threatening, harassing or defamatory messages or other communications in violation of Johns Hopkins policies and/or applicable law;
   b. Sending or posting messages or other communications that appear to come from a party other than the sender, without that party's prior authorization;
   c. Activities that constitute a hostile work environment under Title VII, Title IX, and other applicable laws;
   d. 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;
   e. Broadcast communications to users or JH e-mail systems without the proper institutional or divisional approval, because such communications are subject to approval by designated JH officials;
   f. Use, without specific authorization, of the JH account/e-mail directory (e.g. JHED) for broadcast messages or messaging/social media solicitations.

II. Information Security and Data Protection Policies

Covered Personnel are responsible to help assure the confidentiality, integrity, and availability of the JH Network and IT Resources as well as private or sensitive electronic data. Johns Hopkins has established a number of policies and procedures for protection of its data and IT Resources:

- ICSC Information Technology Security Policies and Standards – these policies are written and approved by the Institutional Computing Standards Committee and cover at both a high level (policies) and in greater detail (Standards and Guidelines) technical security requirements and practices for managing IT Resources and implementing systems.
- HIPAA Privacy and Security Policies – established on behalf of the HIPAA Covered Entities of the university and health system by the JHM Privacy Office, these policies regulate the handling of patient information under HIPAA and related policies.
- Johns Hopkins Personally Identifiable Information Policy – this policy covers handling of a range of private information from highly sensitive financial information to aggregation of less sensitive items such

as addresses and phone numbers. As with the HIPAA Policies above, the PII Policy covers electronic and non-electronic information.

Electronic Information Classification

There are two primary electronic information classifications in the IT Policies: Restricted, which includes Confidential and Internal Use Only, and Unrestricted. Additionally, the terms "sensitive information" and "personally identifiable information" are used in the IT Policies and those listed above as generic characterizations of the contents of certain electronic and non-electronic communications. For purposes of electronic handling, sensitive information should be considered Restricted.

- **Restricted**
  - *Confidential*. This includes information required explicitly by statutory or common law a high level of protection against unauthorized disclosure, modification, destruction, and use. Confidential information includes records protected by HIPAA, FERPA, PCI (credit cards), GLBA (financial services), the Common Rule (human subjects), federal government information policy (e.g. DFARS/FISMA Controlled Unclassified Information [CUI]), U.S. state data breach notification laws and in some cases the laws of other nations.
  - *Internal-use-only.* This includes information that requires protection against unauthorized use, disclosure, modification and/or destruction. Internal-use-only information includes, for example, certain intellectual property (e.g. patent application documents), donor information, budgetary and financial information, security data and internal memos, correspondence, and other documents or information for which distribution is limited as intended by the author and/or administrator. In addition, funding agencies, partners and other stakeholders may have restrictions on the use or distribution of information. Research grants and contracts routinely require security protections, as do operational concerns in finance, auditing, litigation and intellectual property. As privacy law and contractual requirements become more complex, it may be necessary for organizational departments to develop and implement granular privacy and use policies specific to their operational needs.
- **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 information deemed by communicants as sensitive and against unauthorized modification and destruction of information in general. E-mail addresses and phone numbers are generally Unrestricted but may require additional protections if aggregated.

- Not all IT Resources require the same level of security or protection controls. Even within the categories of Restricted and Unrestricted information, appropriate security can vary based on sensitivity and risk. Systems (e.g. hardware, platforms and applications) are deemed Restricted under these policies if they are used to store, transmit or process Restricted information. Security controls should be commensurate with the sensitivity and value of information resources and actual threats to those resources. Covered Personnel 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.

TECH001 Acceptable Use and Security of Johns Hopkins Information Technology Resources

Responsible Executive: Chief Information Security Officer
Responsible Office: IT@JHU Office of CIO
Approved by: Senior Planning Group
Effective: 01/01/2019
Last Revised: N/A

A. **General User Security**

All users of IT Resources have basic responsibilities to help protect the JH Network and themselves. These include protection of their on-line accounts, maintaining their systems and devices at a reasonable level, deploying device security as appropriate, reporting malicious activity and refraining from careless computing practices. These common sense requirements are beneficial to both the user and Johns Hopkins.

When using Johns Hopkins IT Resources, the following security practices are required:

1. Ensure that all devices are up-to-date with IT@JH-recommended security updates and patches for the operating systems and applications, including plugins like Java;
2. Check that computers have current up-to-date anti-virus/anti-malware activated;
3. Use passwords that are difficult to guess and multifactor authentication (e.g., GoogleAuth app to obtain a passcode on a phone) where possible;
4. Minimize storage and transmission of Restricted information, especially to destinations outside the JH Network;
5. Take all prudent steps to avoid loss or theft of laptop computers and mobile devices that are used for Hopkins organizational purposes;
6. For those who may be storing Restricted information (or for anyone associated with Johns Hopkins Medicine) ensure encryption as discussed below;
7. Do not share your JHED password or “tap and go” badge with anyone, and be careful of any communication (e.g. email, text or phone call) that asks for a user password;
8. Beware of unsolicited messages that may be spam or phishing attacks, and be careful with unexpected attachments or links even from individuals that you know;
9. Be wary of unsolicited “support” calls that request credentials or direct a user to download a tool or program;
10. Physically secure your workstation and other computers and ensure that there is an automated time-out and login requiring a password;
11. On JH-owned machines, refrain from installing new software applications except in coordination with professional IT staff;
12. Perform a virus scan on removable media prior to use;
13. Participate in all required security and privacy training and take advantage of other security training and awareness opportunities as those arise;
14. Work with IT staff to ensure that devices and data are disposed of properly (e.g., participate in Hopkins-sanctioned device disposal and recycling programs;
15. Promptly report loss or theft of devices or suspected malicious activity (i.e., see Incident Response Policy below).

    Any device or system, including website or app, that is demonstrating malicious behavior is subject to network shutdown without notice. It is prohibited to maintain a malicious host or application on the JH Network without specific written authorization of the Chief Information Security Officer.

B. **General Network Security**

This section is directed at technical users, especially those outside Johns Hopkins’ central IT administration who are working with network and security tools.

It is Johns Hopkins policy to use appropriate tools and practices to protect the JH Network against intrusion and misuse. Network security requires the cooperation of the entire Johns Hopkins community. In order for JH to ensure an effective security monitoring program, any 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:

1. Using the JH Network in violation of any federal, state, or local law;
2. Attempting to access portions of the JH Network without authorization;
3. Overloading or interfering with the normal functioning of the JH Network or any other network;
4. Using any JH-managed Internet Protocol ("IP") address without authorization;
5. Installing, activating, or configuring any network routing or other device that implements routing protocols (excluding, for example, non-routing switches, hubs, etc.) without prior authorization of the Chief Networking Officer;
6. Install or using a Security Device, performing scanning, "packet sniffing," eavesdropping, or other forms of data interception (including wireless communications) on the JH Network without prior authorization of the Chief Information Security Officer. Third party engagements, projects, or academic courses that may conduct security-related activities must be documented with reasonable specificity regarding purposes and techniques, and such documentation submitted to the Chief Information Security Officer prior to the commencement of these activities;
7. Installing, activating, or configuring a wireless access point without prior authorization of the Chief Networking Officer. The CNO (or designated approval authority) may disallow the registration and operation of an access point if the access point would potentially result in a conflict with wireless service in the same area;
8. Hopkins encourages responsible disclosure of security vulnerabilities to institutional leadership. Such disclosures are considered Restricted information, and public disclosure is prohibited without written authorization from institutional legal or risk management officials. Disclosures should be sent to incident@jhu.edu. Anonymous disclosures should be made to the Compliance Hotline (844-SPEAK2US (844-773-2528).

   Devices that do not have managed encryption solutions may not have access to certain operationally sensitive segments of the JH Network.

C. **Security Responsibilities for Custodians of Restricted Information**

This section applies to custodians of Restricted information. A "custodian" of Restricted information includes any individual who creates, receives or otherwise handles Restricted information as part of their mission-related activity at Johns Hopkins. Occasional handling of Restricted information is enough for an individual to be considered a custodian for these purposes and thus subject to the requirements discussed below. In Johns Hopkins Medicine, all Covered Personnel are presumed to be custodians of Restricted information unless otherwise designated. Accordingly, JHM may have higher requirements for user training, device procurement, access and management.
This section addresses security responsibilities of, and is thus directed towards, general rather than technical users. Users should also refer to the Protection and Handling of PII in the PII Standards [LINK]. Technical discussions are included in further sections below and in the ICSC Security Standards.

1. Authorization – access to Restricted information and systems must be based on appropriate uses. Authorization to access Restricted information must be based on a "need to know," and minimized accordingly.
2. Transmission – It is prohibited to transmit Restricted information across public networks (i.e. the Internet) unless encrypted. Transmission of this type often involves insecure delivery. Examples include but are not limited to:
   a. Emails to non-JH addresses including, for example, gmail, nih.gov, harvard.edu, etc.
   b. Automatic mail forwarding to external systems
   c. Instant messaging across non-JH messaging platforms, including AOL, Trillian, etc.
   d. Unencrypted pagers

   JH has tools for encrypting transmissions, including secure email (http://www.it.johnshopkins.edu/services/email/relay/secure/), instant messaging (https://portalcontent.johnshopkins.edu/TeamCORUS/about.html) and file sharing (http://www.it.johnshopkins.edu/services/collaboration_tools/index.html). Password protection of Microsoft Office attachments is also a sensible protection for transmission of Restricted information to external entities.
3. Mobile Encryption – All laptops and mobile devices, including personally-owned devices, must have full disk encryption installed and activated prior to the receipt or storage of Restricted information. Laptop computers and mobile devices at Johns Hopkins Medicine must be encrypted as a matter of course. As a matter of prudence, any device reasonably likely to be used to store Restricted information should have such encryption activated.
4. Portable Storage Media Encryption – All portable storage media that store Restricted information (e.g. backup tapes, flash drives, DVD's) must be encrypted at the file, folder or device layer to ensure that all Restricted information is protected.
5. Desktop Encryption – storage of Restricted information on desktop computers poses risk of loss or theft. Therefore, desktop computers must have full disk encryption installed and activated prior to the receipt or storage of Restricted information. Desktop encryption is a relatively new requirement, and implementation among divisions and entities may take place in phases. Implementation of desktop encryption at Johns Hopkins Medicine is deemed as high priority.
6. Server Encryption – All servers storing Restricted information (e.g. file servers, email servers, databases) must be stored in a JH-managed or approved data center or otherwise secure area (see Data Center Security Standards and Guidance, http://www.it.johnshopkins.edu/policies/standards.html). Server encryption is advisable for servers in general, and encryption of data-at-rest is required for any server storing Restricted information not located in a data center compliant with ICSC Data Center Security Standards.
7. Cloud Applications – Cloud applications are externally hosted and include technologies characterized by the term Software-as-a-Service and include tools such as Google Apps, Qualtrics, Box, Dropbox, Salesforce, freeconferencecall.com. Use of a cloud service must be coordinated with Hopkins IT and/or division or entity IT leadership in order to ensure that the cloud service meets basic operational and security requirements. It is prohibited to store or process Restricted information using a cloud service without the following: The procurement of cloud applications for Restricted information must be (1) initiated through formal software procurement channels, (2) reviewed by purchasing and/

or legal offices, and (3) appropriate explicit privacy and security protections provisions included in applicable agreements. In addition, there may be requirements for additional assurances such as SSAE 16 SOC 2 or federal (e.g. FISMA, DFARS) certifications. Throughout the life of a Restricted cloud application, it is required that the application maintain a designated project sponsor and ongoing management of system users, interfaces and data. For cloud applications that come under HIPAA, there may be additional requirements for procurement and management.

8. Backup and Recovery – Mission critical systems (recommended for any server-based system) must have documented procedures to create a retrievable, exact copy of critical information and must test data and systems recovery regularly. 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. Certain information may include specific legal requirements for systems back-up and recovery. Unrestricted information is to be backed up as appropriate to the level of risk for loss of information and/or its impact on systems and interfaces.
9. Disposal – Restricted information must be disposed of in such manner as to ensure it cannot be recovered. When donating, selling, transferring, or disposal of computers, removable media and other equipment (e.g. printers, copiers, digital cameras) care must be taken to ensure that Restricted data is rendered unreadable by, for example, defacement, degaussing or other standard techniques. It is usually insufficient to simply “delete” information (or reformat) from most storage media as that information is often easily recovered. JH maintains disposal and recycling agreements with outside firms, and users are encouraged to use these JH-sanctioned services(Data Removal Standards, http://www.it.johnshopkins.edu/policies/standards.html).

D. **General Administration of Systems**

This section applies to all systems administrators, which includes server administrators as well as analysts and developers (e.g., Web developers).

Administration of servers, hosts, devices and applications on the JH Network or using JH IT Resources on other networks requires constant attention to ensuring that systems do not interfere with other JH systems and meet basic security requirements. Compromised systems and applications pose a hazard to the JH Network even if the system or application has no critical data or function.

1. On-boarding servers – Provision of any new server must be coordinated with Hopkins IT and/or division/entity IT leadership in order to ensure that a server meets basic operational and security requirements. In general, a “server” is defined as a computer or computer program that manages access to a resources or service on a network to more than one user or system, and for these purposes also includes virtual and specialized computing platforms.
2. Web presence – Any organizational web presence that invokes an affiliation to Hopkins (institutionally or in part) through words, logos or URL naming must be managed at the university divisional or health system entity level through an approved IT/Web publication group. Divisions and entities may approve departments, centers, programs or individuals to manage websites on a case-by-case basis.
3. Website checklist – All web applications and websites must conduct an internal review consistent with the ICSC Web Security Checklist(http://www.it.johnshopkins.edu/policies/standards.html).

4. Web servers -- Web-sites and Web applications should be documented and reviewed routinely for Web-based vulnerabilities and the possibility of unauthorized access to sensitive information on the Web-site or server.
5. Patch/Update Management – Systems must have controls in place to provide timely notification regarding relevant security updates. Administrators have the responsibility to determine whether and/or when to deploy updates. Administrators must deploy updates in a timely fashion or otherwise document compensating controls.
6. Remote Access – User access from outside the JH Network to JH systems or devices through tools (e.g. RDP, LogMeIn, GoToMyPC, or ssh) must use multi-factor authentication for access and should use a JH-managed VPN where possible.
7. Administration – Administration requires documented privileged authorization procedures, multi-factor authentication, transmission encryption, and regular review of administrator and user access logs.
8. Cloud service provision – In addition to the requirements above, administrators should determine whether a cloud service's security corresponds to sensitivity of information and/or workflows utilizing that service. Administrators are responsible for:
    - Ensuring that there is a clearly designated business owner;
    - Working with an appropriate purchasing department and/or legal office to develop contractual safeguards;
    - Completing the current JH Cloud Vendor Security Checklist(http://www.it.johnshopkins.edu/policies/risk.html
    - Considering data format, retention and destruction requirements;
    - Managing the life cycle of a cloud service, including but not limited to, privacy policies, interfaces, security incidents, data formats, expiration and de-commissioning;
    - Ensuring that Restricted systems utilizing cloud services follow Hopkins IT procedures, including integration where possible with Hopkins IT cloud service offerings.
9. Printers and Copiers – Printers, copiers and other peripheral network-connected equipment should be procured through standard JH-sanctioned vendors and managed according to vendor requirements and guidance. Any external internet access to peripheral equipment must have prior written permission of the Chief Networking Officer. Storage media on these devices are generally deemed as portable equipment and thus should be encrypted where possible and physically secured. Disposal of this equipment should follow the disposal requirements in K.9 above.
10. End-of-life –It is the administrator's responsibility to manage a system or application's product and support life cycle and ensure that systems are "sunsetted" consistent with mission objectives and the availability of support. Unsupported and/or out-of-date systems are a common, preventable risk on enterprise networks, the mitigation of which requires some coordinated planning between administrative and IT management.
11. Systems monitoring – A critical piece of administering systems and applications involves systems monitoring. Systems monitoring processes should comply with the following:
    - All monitoring, data collection and investigations are to be undertaken in a professional and discreet manner;
    - Data collected and stored must meet the general privacy standard of "minimum necessary" to accomplish specific mission objectives. It should also be minimally invasive of user activities;

- User information beyond what can be found in a typical JHED listing (including for example use patterns, like browser history) should be considered sensitive, including information regarding use of IT Resources;
- While it is important that monitoring and security teams collaborate with each other and other IT staff, this must be balanced against potential confidentiality considerations;
- Use of investigation tools should be logged, monitored and routinely audited. Any changes in data collection techniques or in data elements collected must be placed into appropriate change control;
- Routine logging and analysis is generally presumed to be appropriate when in compliance with the requirements outlined here. Extraordinary collection, sharing and/or use of sensitive information should be approved by division/entity management.

E. **Security Administration of Restricted Servers and Applications**

This section applies to systems administrators of business-critical systems.

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

As the purpose and functions of systems vary, administrators (including but not limited to, those for networks, hosts, applications, devices, databases and interfaces) should refer to specific JH Standards for guidance and industry best practices. Administrators must follow ICSC standards regarding server and application configuration and administration, including:

1. 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. All Restricted servers must be registered in the Hopkins IT Configuration Management Database (CMDB) and maintain continuous registration.
2. 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 mission objectives.
3. Authentication – Restricted systems and applications that are accessible outside the JH Network should be authenticated through multi-factor authentication, including but not limited to the JH Virtual Private Network (VPN).
4. Administration – Systems administration may only be performed by authorized, trained personnel. Servers and applications that process or store Restricted information must meet applicable security requirements.

5. Data Security – Encryption of data-at-rest is required for Restricted servers that are not located in a Hopkins IT data center.
6. Vulnerability Scanning – There should be routine monitoring and remediation of vulnerabilities, specifically regarding components connected to the JH Network. JH maintains tools for server and other asset scanning (http://www.it.johnshopkins.edu/restricted/security/jhsc.html).Training and Awareness – technical and operational management should pair electronic system access with training that includes security awareness. Technical staff should include security as part of on-going skills development.

F. Security Administration Of Restricted Devices

JH Policies are principally concerned with mitigating risk from compromise of Restricted information or workflows. A "Restricted Device" is any computing device that is used for storage, transmission or processing of Restricted information. The application of policy weighs inherent risk associated with a device more heavily than the provenance or ownership of that device. Therefore, a personally-owned computer that is used to store Restricted data is generally of greater concern to these policies than a JH-owned workstation in a non-critical setting. While it is realistic to acknowledge that personally-owned devices are used for Restricted purposes, JH discourages such use, as these devices may have non-standard configurations and thus be unsuitable for appropriate security controls. In such cases, it is the users responsibility to implement compensating controls such as use of virtualized desktops.

All Restricted Devices must have the following controls:

1. Configuration and management – Restricted Devices should be managed to professional standards, by trained JH staff with sufficient knowledge and resources to ensure that data on them are properly secured. Avoid providing users with administrator access. Operating systems and network-aware applications must be patched and maintain automated virus detection and update mechanisms.
2. Services – Restricted Devices should not run programs or services that are unnecessary to Hopkins' mission purposes. Network-aware client software, such as Web browsers or email readers, should block the automatic execution of attachments, graphical files, or other common carriers of malicious code.
3. 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.
4. System 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.

G. **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 division and entity is required to develop, maintain, implement, and adhere to plans and

procedures for disaster recovery and business continuity according to its own academic and mission 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:

1. Loss of IT personnel
2. Loss of local resources
3. Loss of the work facility
4. Loss of IT connectivity
5. 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 division or 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.

H. **Ownership of and Administrative Access to JH Network**

The JH Network is Johns Hopkins' private property and Johns Hopkins reserves the right, under certain circumstances, to access, restrict, monitor the JH Network and contracted networks and regulate the systems that support and contain them. This includes access without notice, where warranted. E-mail and user accounts and their contents on the JH Network are generally treated as private by Johns Hopkins. It is not the routine practice of JH IT administrators to view or disclose the content of others' electronic files, but Johns Hopkins reserves the right, and may be legally required, to access, copy, examine, and/or disclose all files stored or processed by JH IT Resources and/or transmitted on, across, or through the JH Network, 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 Johns Hopkins' rights or property. For these reasons, there should be no presumption of privacy or confidentiality concerning information stored on or processed by JH IT Resources and/or transmitted on, across, or through the JH Network.

TECH001 Acceptable Use and Security of Johns Hopkins Information Technology Resources

Responsible Executive: Chief Information Security Officer
Responsible Office: IT@JHU Office of CIO
Approved by: Senior Planning Group
Effective: 01/01/2019
Last Revised: N/A

I. Access Control for JH IT Resources

Only authorized users should have physical, electronic or other access to JH 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. To meet these objectives, we strongly encourage that access management leverage Hopkins' managed enterprise directories. Administrators and managers are primarily responsible for establishing, documenting and managing access control policies and processes for their IT Resources.

1. ***Authorization***

   Authorization of access to IT Resources must be based on appropriate mission uses. Access privileges must be reviewed and revised as appropriate. 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 should 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.

2. ***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, which is defined as authentication that does not rely on a password alone (i.e. multi-factor authentication.

   Individual 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). Managers/supervisors may not require or request individual passwords from subordinates. 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. Users may not access IT Resources through another user's account.

   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:

   a. Unique User IDs
   b. 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. Passwords should be supplemented with additional authentication where possible (e.g. enterprise multi-factor authentication, certificates or browser cookies)
   c. Lock user accounts after five to ten (5 - 10) unsuccessful login attempts
   d. Forced periodic password changes every 180 days unless there are other factors deployed in authentication. There may be specific sponsor or regulatory requirements for more frequent password changes, and those requirements should be followed as possible
   e. Restrictions on password re-use

f. Banners – On login include banners advising users that systems and/or applications 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.
g. 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.
h. 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 services. Server applications that use enterprise credentials for authentication should not collect or cache those credentials.

3. Prevention and Detection of Unauthorized Access – 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 :
   a. 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.
   b. 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.
   c. 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.
4. Systems logs should be treated as sensitive and appropriate measures taken to ensure log integrity, appropriate retention periods and that access is limited to those with a "need to know." This is especially important for cloud services where systems/service owner log monitoring plays such a critical role in the security posture, see the JH Logging Standards and Guidance.

J. **Data Center Security**

JH 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. (see Data Center Security Standards and Guidance, http://www.it.johnshopkins.edu/policies/standards.html):

1. Data centers that store, process and/or transmit Restricted information must have physical access controls commensurate with the level of risk and must include 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.

2. Facilities with network equipment or a small number of Restricted servers or devices must have physical access controls commensurate with the level of risk and must include all of the following: (1) card-swipe entry devices with access logs, (2) access alarms (e.g. to check for propped doors). It is recommended that guards, video surveillance and hardware monitoring tool be used also.
3. To protect against environmental hazards to any system, power, temperature, water and fire monitoring devices are to be deployed as appropriate.

K. Third-Party Vendor Relationships

1. *General Vendor Responsibilities*

Third-party 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. Authorization of vendor access requires that Hopkins systems owner document reasons for vendor access and a general account of how such access will be granted during maintenance.

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.

2. *Vendor Access to JH IT Resources*

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 mission 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. Remote electronic access to IT Resources requires multi-factor authentication
i. Vendor access to JH IT resources may be re-certified annually.
j. Violations of this policy may result in the loss of vendor access to JH IT Resources and/or other legal or contractual recourse.

L. **Incident Response And Recovery**

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 (incident@jhu.ed).

b. Physical Security Reporting -- Incidents that principally involve theft, destruction, and/or other illegal activity related to IT Resources should be reported Corporate Security http://www.hopkinsmedicine.org/security_parking_transportation/about_us/contact_us.html.

Security departments coordinate with the JH-CIRT to investigate and evaluate potential compromises of networks and sensitive information.

Exceptions/Exclusions

JHU Applied Physics Laboratory

Policy 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.

Violations*[optional]*	*It is an explicit violation of this policy to do any of the following:* *[To be completed]*
Enforcement	*The [appropriate office of the University] will investigate suspected violations, and may recommend disciplinary action in accordance with University codes of conduct, policies, or applicable laws. Sanctions may include one or more of the following:* • *suspension or termination of access;* • *disciplinary action up to and including termination of employment;* • *student discipline in accordance with applicable University policy;* • *civil or criminal penalties.*
Reporting Violations	*[Specifics depend on policy content and suspected violators (i.e., student violations reported to Student Affairs, etc.)]*

Related Resources

See Section II Information Security and Data Protection Policies

Contacts

Subject Matter	Office Name	Telephone Number	E-mail/Web Address
IT Policy	Information Technology	410-735-4477	itpolicy@jhu.edu
Computer Security Incidents	Information Technology	410-516-4357	incident@JHU.edu

TECH001 Acceptable Use and Security of Johns Hopkins Information Technology Resources

Responsible Executive: Chief Information Security Officer
Responsible Office: IT@JHU Office of CIO
Approved by: Senior Planning Group
Effective: 01/01/2019
Last Revised: N/A

Approved By

Institutional Computing Standards Committee

https://it.johnshopkins.edu/about/committees/icsc