

**POLICY TITLE: USAGE OF HOSPITAL IT RESOURCES**

**APPROVED BY: CHIEF INFORMATION OFFICER**

**ORIGINATED BY: INFORMATION SECURITY OFFICER**

**DATE: 08/29/08**

---

**POLICY:**

Information is an extremely valuable resource that The Christ Hospital ('TCH') and its affiliated companies, including providers, referring providers, educators, students, service vendors and contractors, hereinafter collectively referred to as 'Hospital', depends upon to conduct business. Proper use of Information Technology (IT) Infrastructure is necessary to foster and grow the information environment which, in turn, allows Hospital employees to more effectively perform their jobs.

This policy is intended to define proper use of all IT infrastructure resources, including computer hardware and software tools, office and cellular telephones, electronic mail, internet usage, and other IT resources.

The Hospital's IT systems and networks are to be used in the furtherance of Hospital business. No Hospital employee, provider, referring provider, educator, student, service vendor, contractor, or partner should use these electronic resources to espouse personal, political, or religious views or to solicit support for any cause or event not associated with The Christ Hospital. It is the responsibility of each individual to utilize the Information Technology infrastructure resources in a responsible, ethical, and lawful manner.

**RESPONSIBILITY:**

This policy applies to all IT Infrastructure owned and/or managed by the Hospital, on Hospital premises, in virtual offices or homes, at customer sites, or elsewhere. In addition, this policy applies to activities that occur during an employee's standard work day and "non-business hours" as well.

It is the responsibility of every employee and affiliate of The Christ Hospital, including providers, referring providers and contractors to (1) read, understand, and adhere to the provisions in this document, (2) report violations of this policy as appropriate, and (3) safeguard information resources commensurate with the sensitivity, nature, and value of that resource. Hospital managers are accountable for disseminating the policy, guiding employees and contractors, assuring adherence, and taking corrective/disciplinary actions as needed.

**DEFINITIONS**

**FOR INTERNAL USE ONLY:** This information is not intended for public release.

**BLOG** – A blog (a contraction of the term "Web log") is a Web site, usually maintained by an individual, with regular entries of commentary, descriptions of events, or other material such as graphics or video.

**IT RESOURCE** – A Hospital IT Resource is any computer, electronic equipment, or software program owned or managed by TCH or used to conduct Hospital business.

**TROJAN** – A Trojan horse, also known as a trojan, is malware that appears to perform a desirable function but in fact performs undisclosed malicious functions. Therefore, a computer worm or virus may be a Trojan horse.

**WIKI** – A wiki is a collection of web pages designed to enable anyone who accesses it to contribute or modify content, using a simplified markup language. Wikis are often used to create collaborative websites and to power community websites. For example, the collaborative encyclopedia Wikipedia is one of the best-known wikis.

**PROCEDURE:**

**This policy covers the following areas:**

- A. **General**
- B. **Internet Access**
- C. **Electronic Mail**
- D. **Personal Computers and Electronic Storage Media**
- E. **Voice Communications and PDA**
- F. **Global Remote Access (Citrix)**
- G. **Web Servers**
- H. **Usage of Blogs, Wikis, and discussion forums**
- I. **Compliance Requirements**

**POLICY STATEMENTS**

**A. General:**

1. Electronic information exchange consists of letters, memos, files, news, voice, and data generated by various applications; sent to, sent from, or solicited by, Hospital employees through Hospital owned or managed networks or provided by any third party sources.

2. The Hospital's IT infrastructure system can be used to distribute company-related information such as company supported charitable fund drives, information on Hospital activities, available resources, professional development conferences, etc. All such items must be approved by the TCH Marketing department and/or the TCH Human Resources department.
3. Any Hospital employee who receives or views harassing or inappropriate information via Hospital IT resources should report the incident to the TCH Information Security Officer immediately.
4. Usage requirements for select IT tools are provided below. This policy does not and cannot address every IT infrastructure situation. In all cases, Hospital employee conduct should be based on good judgment and the Hospital's EXCEL core values. When in doubt, employees should also seek guidance from their manager.
5. System access (e.g. Citrix account, Epic or Lawson application account) is granted for individual Hospital employee use only. Users must not share a login information or associated password, and/or instructions for access to the Hospital's infrastructure with anyone.

**B. Internet Access:**

1. The use of IT resources to access any service on the public Internet, including the World Wide Web (WWW), is reserved for Hospital employees, providers, referring providers, educators, students, service vendors and contractors, for the direct support of legitimate Hospital business objectives.
2. Usage of the Hospital's Internet service is monitored. TCH maintains filtering and monitoring software which prevents access to locations on the Internet that are clearly not related to business. The ability to connect to non-business sites does not in itself imply acceptable business use. When access to a restricted site is attempted, a log entry is created which identifies the user and the site being accessed. These log files are retained and may be forwarded to the user's manager for appropriate action. Use of any external Internet resource, such as proxy software, anonymizers, or onion-routers, in an attempt to circumvent Hospital filtering or monitoring devices is prohibited.

3. Material that conflicts with the Hospital's EXCEL core values and/or is not compatible with a productive work environment must not be viewed, downloaded or accessed in any way. Access to such materials can result in potential legal liabilities to the Hospital. Workers must not access materials that may be offensive to others and must disconnect immediately upon discovering they have connected to such sites.

Examples of restricted sites and material include, but are not limited to those with information or activities such as pornography, criminal skills and illegal activities (including those related to the circumvention of network security controls), unauthorized copies of licensed software, dating services and discussions, the purchase and use of illegal or recreational drugs, extreme or obscene material, gambling, hate speech, sports, listening or playing music (e.g. MP3), games, and entertainment.

4. Non-business use of the Hospital's systems, networks, or Internet connection for online auctions, home-based businesses, chat groups, and entertainment-related streaming audio / video impacts network resources available to legitimate Hospital applications and is prohibited.
5. If access to a blocked web site is necessary to conduct business-related activities, the employee's manager must provide a clear written business reason to the TCH Information Security Officer to enable the employee to gain access.
6. Use of the Hospital's systems, networks, or Internet service to penetrate, assess, or attempt to penetrate the security of another organization is prohibited, except as authorized by the TCH Information Security Officer. Such activity includes, but is not limited to, the use of port scanners, exploitation toolkits, and other network identification and penetration software.
7. "Hacker" type hardware and software tools (e.g., packet filters, packet sniffers, password crackers, etc.) must not be used on any equipment connected to the Hospital's Network without written authorization from the TCH Information Security Officer. Such tools include but are not limited to those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or scan configuration of infrastructure components. Hardware or software tools that could be employed to evaluate or compromise information systems security must not be used on or in conjunction with any Hospital resources unless specifically authorized in writing by the TCH Information Security Officer.
8. Connections between the Hospital IT infrastructure and the Internet implemented without the full knowledge and consent of IT Services and the TCH Information Security Officer are prohibited and subject to immediate disconnection.

9. Connection of unauthorized networking devices not issued by TCH, such as network hubs, wireless routers, etc. is prohibited. Any unauthorized devices connected to the Hospital network are subject to immediate disconnection and/or confiscation.

**C. Electronic Mail (E-mail):**

1. Creating or exchanging offensive, harassing, obscene or threatening messages is prohibited.
2. Refer to policy # 4.24.104 "Data Encryption" for encryption guidelines when transmitting electronic copies of any confidential or EPHI data.
3. E-mail must not be used to create, forward, or respond to advertisements, solicitations, chain letters and other unsolicited non-business related e-mail.
4. Use of e-mail resulting in a violation of copyrights is prohibited.
5. The content of a message or attachment that belongs to another user must not be altered in a manner designed to imply the original user intended to send the altered message.
6. E-mail accounts may be granted only to Hospital employees, board members, providers, educators, students, service vendors, or contractors and only by the IT Services organization.
7. E-mail systems and messages are considered Hospital property and are intended for business use only. TCH reserves the right to monitor and audit e-mail system usage and message content. No expectation of privacy should be maintained by e-mail system users. Hospital management may review the content of e-mail messages at any time.
8. Automatic forwarding of Hospital business e-mail to a personal Internet Service Provider account is prohibited.
9. Hospital personnel must not access "free" external web mail accounts (e.g. Google Gmail, Yahoo mail, Microsoft Hotmail) from the Hospital's private network.
10. Hospital personnel must not access non-business social networking sites (e.g. Facebook, Myspace) from the Hospital's private network.

**D. Personal Computers and Electronic Storage Media**

1. Storage of EPHI data on unencrypted removable media, including but not limited to CD / DVD, USB removable flash drives or hard drives, floppy disks, etc. is prohibited unless authorized by the TCH Information Security Officer.
2. EPHI data may be stored on removable media provided either 1) the device provides encryption capability via AES or other strong encryption algorithm, or 2) the data is encrypted prior to storage using AES or other strong algorithm (e.g. using PGP or encryption software).
3. Hospital employees using hospital-issued laptops must take reasonable precautions to protect the equipment from theft. Reasonable precautions include not leaving the device unattended in a vehicle, usage of a Kensington cable security lock, etc.
4. Installation of unapproved software on any Hospital system is prohibited. This includes, but is not limited to, game software, file sharing programs (e.g. LimeWire, Napster), remote control software (e.g. PCAnywhere, GotoMyPC, LogMeIn), etc. A listing of approved software products is maintained by IT Services.

**E. Voice Communications and PDA (i.e. Mdata, Blackberry):**

1. Telephones, associated analog or digital lines, fax machines, and voice mail boxes are the sole property of the Hospital and are reserved for Hospital use only. Access may be revoked at any time.
2. Hospital business-provided cellular phones, pagers, and other equipment are the sole property of the Hospital and may be revoked at any time. Lost or stolen devices must be reported immediately so that service can be terminated eliminating the risk of unauthorized use.
3. Hospital provided cellular phones and other devices are intended for business use only.
4. Employees who use a cellular phone or pager in performing their job functions must do so in a safe and prudent manner. A hands-free device (e.g. Bluetooth headset) must be used whenever possible when talking on a cellular phone while operating a vehicle.

5. If a hands-free device is not being used while the employee is operating a motor vehicle, the vehicle must be stationary and in a "park" position before initiating a cellular call or responding to a page. Cellular phone use without a hands-free device is not permitted in a moving vehicle, regardless if the vehicle or the phone is personally owned or leased by the Hospital for business use. If a cellular call is received while an employee is operating a motor vehicle, the employee should either pull over onto the shoulder of the road and place the vehicle into "park", or preferably drive to an appropriate parking location and place the vehicle in "park", prior to engaging the phone call. Hospital provided phones are intended for business use only. However, this policy applies to any cellular call relating to the employee's job duties, whether placed or received on a Hospital-provided phone or a personally-owned phone.
6. TCH may set monetary limits on monthly charges for business-related cellular expenses. Expenditures over the set monetary limits must be approved by TCH management.
7. All mobile computing devices issued by the Hospital or used to store Hospital data, e.g. PDAs, Mdata handhelds, and Blackberrys, must have a password on the device. This password should be known only to the user. The device should have auto-lockout or auto-wipe capability that will render the device unusable after a maximum of 20 failed login attempts.

**F. Global Remote Access (Citrix):**

1. Global Remote Access is made available to Hospital personnel via the TCH Citrix environment. Citrix accounts are the sole property of the Hospital and may be revoked at any time and for any reason.
2. Utilizing Citrix to gain access to the Internet for non-business purposes is not permitted at any time. Any access to the Internet must be for business reasons whether it is during or after working hours.
3. Hospital employees, providers, referring providers, educators, students, service vendors and contractors, and business partners must connect to the Hospital's infrastructure only through approved methods provided by IT Services. Unauthorized connections to the Hospital's infrastructure or attempts to circumvent Hospital security measures are prohibited.
4. Hospital employees, providers, referring providers, educators, students, service vendors and contractors who utilize a Virtual Private Network (VPN) / broadband connection to access the Hospital network must install an approved personal firewall and configure it to Hospital security specifications.

5. Hospital employees using VPN to connect to the Hospital's network must power off machines connected to cable modems or digital subscriber lines (DSL) when not in use. This is particularly important when leaving your workstation unattended for extended periods of time, such as overnight and on weekends.
6. Use of remote administration products must adhere to IT Services processes, standards, policies and procedures.
7. Hospital data must be protected by the Hospital IT infrastructure. Public Internet Service Providers (ISP's) are not to be used to transmit confidential Hospital information or EPHI data without encryption; nor, should they be used to store sensitive Hospital information. ISPs are not considered secure.

**G. Web Servers, Web Sites, and Web Content:**

1. All Hospital web servers must be set up, configured, and maintained by IT Services. Interceptor web servers/sites for the purpose of intercepting or altering content are prohibited.
2. Web sites must not be linked to non-Hospital sites that are not business relevant.

**H. Usage of Blogs, Wikis and other Web 2.0 technologies:**

1. Posting of EPHI data to any external blog, wiki, or other public discussion forum is strictly prohibited and will result in immediate disciplinary action as indicated in the "Compliance Requirements" section of this policy.
2. Posting of Confidential or Internal Use Only data about Hospital processes, policies, or operations to any non-business-related external blog, wiki, or other public discussion forum is prohibited.
3. Posting tainted software, i.e., containing known Trojan horses or viruses, to any discussion internal or external discussion forum is prohibited.
4. Postings reflecting unprofessional behavior, including but not limited to profanity, vulgarity, defamatory remarks, racist or sexist remarks or anything that violates the TCH EXCEL core values to any internal or external discussion forum is prohibited.
5. Postings to solicit/simulate chain mail-like scheme(s) are prohibited.
6. Any use that results in a violation of copyright or intellectual property rights is prohibited.

7. Revealing personal information about Hospital employees in any internal or external discussion forum is prohibited.

**I. Policy Compliance Requirements:**

1. TCH reserves the right to monitor, audit, and disclose, without permission from the user, information regarding usage of any Hospital system and/or any electronic data generated and stored using the Hospital's IT resources to ensure policy compliance unless prohibited by law.
2. Attempts, whether successful or unsuccessful, to circumvent Hospital security processes, controls, or technology may result in loss of access to IT resources and/or disciplinary and/or legal action as defined below.
3. TCH Business Partner Organizations (e.g. providers, referring providers, educators, students, service vendors, contractors) failing to comply with the provisions of this policy may be disconnected from the TCH network. Once disconnected, the organization shall not be reconnected to the TCH network until policy compliance has been verified by TCH.
4. Individuals failing to comply with the provisions of this policy are subject to loss of access to IT resources and/or disciplinary action up to and including dismissal. In addition, violations of this policy may result in legal action, including injunctive relief and civil damages, and/or criminal prosecution.