HOUSTON Methodist LEADING MEDICINE

Policy IM01

Subject:
Acceptable Use of Computing Resources

Applies to:
All Users, All Entities

Originating Area:
Information Technology Division

Effective Date:
July 2004

Date Revised/Reviewed:
October 2013

Target Review Date:
October 2016

POLICY STATEMENT

Computing resources of Houston Methodist and Internet access are available to all authorized users. These resources consist of computing devices that are owned by Methodist and/or connected by any method to Methodist in order to gain access to the Internet, e-mail or any other applications and systems administered by Houston Methodist. The Internet enables worldwide connection to electronic mail, discussion groups, databases, software and other information resources. Houston Methodist firmly believes that computing resources are vital to conduct business. Access shall be used to improve patient care and operations consistent with the goals and values of Methodist.

IMPLEMENTATION

AVAILABILITY OF ACCESS:

User Orientation:
Appropriate use of Houston Methodist computer resource will be discussed during employee orientation.

Privilege:
Access to Methodist computing resources is a privilege, not a right. Any system user identified as a security risk or having violated this Acceptable Use Policy may be denied access to resources.

Subject to Monitoring:
All computing resource usage, including Methodist issued Mobile devices, shall not be considered personally confidential and is subject to monitoring at any time to ensure appropriate use.

User Responsibility:

- Users are responsible for their actions in accessing and using available resources.
- Users are required to maintain password confidentiality and not share passwords with others.
- Ethnic, racial, vulgarity and any other inflammatory language are prohibited.
- Users are responsible for complying with copyright laws.
- Users are responsible for securing electronic mail that contains confidential patient, employee, or financial/business data by typing **secure mail** in the subject line.
- Users are responsible for notifying the appropriate supervisor if they should encounter any material or electronic communication that is inappropriate.

INAPPROPRIATE USE:

Inappropriate use includes, but is not limited to, those that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of any components connected to Houston Methodist network. The following actions are considered inappropriate uses and are prohibited:

Violations of Law: Transmission of any material in violation of any U.S. or state law is prohibited. This includes, but is not limited to: copyrighted material; threatening, harassing, or obscene material; or material protected by Methodist. Any attempt to break the law through the use of Methodist resources may result in disciplinary action or litigation against the offender by the proper authorities. If such an event should occur, Houston Methodist will fully comply with the authorities to provide any information necessary for investigation and/or for the litigation process.

Modification of Computing Devices: Modifying or changing device settings and/or internal or external configuration without appropriate permission is prohibited.

Electronic Mail Violations: Forgery of electronic mail messages is prohibited. Reading, deleting, copying, or modifying the electronic mail folders of other users, without appropriate permission is prohibited. Sending unsolicited junk mail; chain letters; political lobbying; and/or ethnic, racial, vulgar or obscene messages or pictures is prohibited. Electronic mail that contains confidential patient, employee, or financial/business data must be secured by typing **secure mail** in the subject line. Failure to do so is prohibited.

File and Data Violations: Deleting, examining, copying, or modifying files and/or data belonging to other users, without appropriate permission, is prohibited. Storing patients' personal health information (PHI) and personal identifiable information on an unsecured shared computing resource (e.g., shared drive) or a mobile computing device (e.g., thumb drive and laptop) is prohibited unless PHI is stored in a manner that can be properly secured.

Copyright Violations: Downloading or using illegally obtained copyrighted information is prohibited.

System Interface and Alteration: Deliberate attempts to exceed, evade or change resources without authorization are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

PCI-DSS, Payment Card Industry (PCI) Data Security Standard**:** The sending of unencrypted Primary Account Numbers (PANs) associated to any credit card, via any messaging system (including e-mail, instant messaging, chat rooms,) is prohibited.

WARNING AND DISCLAIMER:

Web sites accessible through Houston Methodist computing resources including electronic mail received from the Internet, commonly known as spam, may contain material that is illegal, defamatory, inaccurate or controversial. Methodist makes every effort to limit access to objectionable material. However, controlling all such materials is impossible. This policy applies to standalone devices as well as devices connected to its network.

COUNCILS OR COMMITTEES REVIEWING OR APPROVING PROCEDURE

Information Security and Privacy Committee (ISPC)

AUTHORITATIVE REFERENCES

Data Security Standard (DSS).

NAME OF APPROVING EXECUTIVE: Marc L. Boom, M. D.
TITLE: President,
Chief Executive Officer

(Signed original on File)

____
Signature of Approving Executive

____
Date Signed