East Jefferson General Hospital
Metairie, LA 70006

Administrative Policy And Procedure
Policy No. IT-7
Page 1 of 4
Effective Date: August 1, 1997
Approved by:

Title: **INTERNET ACCESS**

ORIGINAL SIGNED BY DR. PETERS
Mark Peters, MD, President and CEO

Revised: 9/1/99, 2/2000, 4/2003 (H); 10/13

I. POLICY:

The Hospital provides Internet access to designated management/technical staff for business-related purposes, to communicate with customers and suppliers, to research relevant topics, and obtain useful business information.

II. DEPARTMENTS AFFECTED:

All Hospital Departments and Medical Staff.

III. DEFINITIONS:

Internet Firewall: A security system that protects the Hospital from unauthorized access through the Internet.

IV. GUIDELINES:

A. The Hospital provides access to the vast information resources of the Internet to help Team Members do their jobs faster and smarter, and be well-informed business citizens.

B. Team Members will conduct themselves honestly and appropriately on the Internet and respect copyrights, software licensing rules, property rights, privacy, and prerogatives of others just as with any other business dealings. All existing Hospital policies apply to such conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of Hospital resources, sexual harassment, information and data security, and confidentiality.

C. All Team Members granted Internet access with Hospital facilities will be expected to follow the provisions of this and related policies. Team Members should review the Internet Access Manual prior to accessing the Internet. This manual is available electronically attached to this policy.

V. PROCEDURES:

A. Authorization for Access:

The procedure to gain Internet access shall be as follows:

1. Team Member requesting access to the Internet via a Hospital computer must complete and sign a System Access Management (SAM) Request Form.

2. The request must be approved by the Director and submitted to Information Technologies.

3. Completed SAM Requests will be submitted through the Help Desk.

4. Team Members granted access will follow all guidelines and procedures as stated in this policy and the *Internet Access Manual*.

B. Management and Administration:

1. The Hospital has software and systems in place that can monitor and record all Internet usage and reserves the right to do so at any time. No Team Member should have any expectation of privacy with regard to Internet usage.

2. The Hospital reserves the right to inspect any and all files stored in private areas of the network in order to assure compliance with policy.

3. The display of any kind of sexually explicit image or document on any Hospital system is a violation of the policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using Hospital network or computing resources.

4. The Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any Hospital resources for illegal activity is grounds for immediate dismissal.

5. Internet access will be limited to those Team Members who have a legitimate business need.

6. Team Members with Internet access may not use Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.

7. Team Members with Internet access may not use Internet facilities to download images or videos unless there is an explicit business-related use for the material.

8. Team Members with Internet access may not use Internet to download any software to Hospital computers without obtaining written authorization from Information Technologies Division. A request for authorization must be submitted to the Help Desk by the Director of the department requesting authorization.

9. Team Members with Internet access may not upload any software licensed to the Hospital or data owned or licensed by the Hospital without explicit written authorization from Information Technologies Division. The Director of the requesting department must submit a request for authorization to the Help Desk.

10. Any personal use of the Internet is subject to all the provisions of this and related policies. In addition to the foregoing constraints and conditions, such use does not: (i) directly or indirectly interfere with the Hospital's operation of computing facilities; (ii) burden the Hospital with noticeable incremental cost; or (iii) interfere with the email user's employment or other obligations to the Hospital. Any questions are to be directed to the User's supervisor/representative.

C. Confidentiality:

User ID's and passwords help maintain individual accountability for Internet resource usage. Any Team Member who obtains a password or ID for an Internet resource must keep that password confidential. Hospital policy prohibits the sharing of user ID's or passwords obtained for access to Internet sites except for enterprise wide supported memberships.

D. Security:

1. All Hospital computers that connect to electronic services outside of the Hospital's network must use our Internet access link.

2. Only those Internet services and functions with documented business purposes for this Hospital will be enabled at the Internet firewall. Hospital network security policy requires that certain transactions and downloads be blocked at the outermost firewall. However, users with a specific business need for blocked access may request such access with business approval through the Help Desk.

VI. <u>VIOLATIONS</u>:

Refer to Human Resources Policy D-1, Discipline Policy.

VI. RESPONSIBILITY:

Questions regarding this policy and recommended revisions shall be directed to the Chief Information Officer or designee.

VII. REFERENCE:

Human Resources Policy:
D-1 “Discipline Policy”

VIII. ATTACHMENT:

Internet Access Manual