

**ST. LUKE’S-ROOSEVELT HOSPITAL CENTER
HUMAN RESOURCES POLICY AND PROCEDURE MANUAL**

Section/Policy Number: Administrative - #1002		
Subject: Computer and Communications Security Policy		
Effective Date: 3/2000	Revised Date: new	Supersedes: n/a
Date Reviewed: 3/2003		
Distribution: Human Resources Policy and Procedure Manual Holders		

Purpose: This Policy clarifies and codifies the rules for the use and protection of St. Luke’s-Roosevelt Hospital Center’s computer and communications systems. This Policy applies to everyone who works at or for the Hospital Center including employees, consultants, independent contractors and all other persons who use or have access to these systems.

Policy:

1. All Hospital Center computer systems, telephone systems, voice mail systems, facsimile equipment, electronic mail systems, Internet access systems, related technology systems, and the wired or wireless networks that connect them are the property of the Hospital Center and should be used for business purposes only.

2. All information and documents created, received, saved or sent on the Hospital Center’s computer or communications systems are the property of the Hospital Center. Employees have no personal privacy right in any material created, received, saved or sent using Hospital Center communication or computer systems. The Hospital Center reserves the right to access and disclose such material at any time without prior notice.

3. The use of the Hospital Center’s computer or communications systems to send discriminatory or harassing messages or material and the use of vulgarities, obscenities, foul or abusive language is prohibited.

4. The Hospital Center’s computer and communications systems should not be used to solicit or proselytize others for commercial ventures, political or religious causes, outside organizations (including philanthropic organizations but excluding Hospital Center sponsored campaigns such as for United Way) or for other non-job-related purposes.

5. Unauthorized accessing or disclosure of stored communication or computer files by a Hospital Center employee is a violation of Hospital Center policy.

Electronic Mail Usage /Internet Access

All e-mail communications should be written with the same care and judgment as would be the case for memoranda or letters written on Hospital Center letterhead and with the expectation that they may be reviewed by third parties. The Hospital Center may preserve all e-mail messages, even after they have been “deleted”, on magnetic media for some period from the date the message is created. Periodically, all electronic media copies of the e-mail message will be deleted. If the e-mail is relevant to a legal record-keeping requirement or may be of some other administrative or historical relevance, the message should be printed and filed in an appropriate file. If the Hospital Center becomes involved in an investigation, litigation or any other proceeding which may necessitate the review or production of Hospital Center records, the Hospital Center may suspend the regular deletion of all or part of e-mail messages for an indefinite period without notice. Employees may not download files from the Internet without appropriate approval.

Voice Mail

The Hospital’s Center’s voice mail system is to be used only when employees are not able to answer the phones for which they are responsible. Voice mail should not be used on a regular basis or to screen calls. Voice mail messages should ordinarily be deleted after review by the intended recipient. If there is a reason to retain a particular voice mail message, an employee should telephonically archive the voice mail message.

Telephone Services

Unauthorized personal telephone calls during working time and the placement of a personal long distance telephone call at the Hospital Center’s expense are prohibited.

Computer Operations and Data Communication

1. Unauthorized access to areas containing telecommunications and data communications equipment is prohibited.
2. The Information Services Department (IS) authorizes the operation of back-ups of the data files on the Hospital’s computers on a regular basis. If a “restore” of a file is necessary, IS should be contacted.
3. As confidential information will be transmitted through the Hospital’s data communication networks, all reasonable precautions to protect that security have been taken. Any attempt to breach that security shall be grounds for disciplinary action or dismissal. Any employee who believes that the security of the data communications system has been breached must report that breach to his or her supervisor immediately.

4. Copying of a computer program or its documentation is an infringement of the copyright rights of the owner. The unauthorized copying of computer software, a copyright infringement, is punishable by civil and criminal penalties.

5. When an employee is terminated or leaves the Hospital Center's employ, that employee's access to the hospital computer systems and electronic data shall be terminated. When it becomes necessary to involuntarily terminate a person's employment, IS must be notified in advance of such termination. From the point of time when an employee is advised of dismissal, no further access to the computer systems will be permitted.

6. Contracts with vendors for hardware, software, maintenance services, or data - including contracts relating to personal computer application -- may only be executed through IS, Continuum Services Corporate Purchasing Department, and the Legal Department.

7. All employees have an obligation to preserve the trade secrets of their prior employers. Employees should therefore never bring in, use, or copy software or related documentation, or any other trade secrets developed at or owned by prior employers, nor may they take or use such material obtained in connection with Hospital Center employment in any subsequent employment.

Protection of Electronic Data and Information

All employees are responsible for taking appropriate steps to safeguard the Hospital Center's confidential electronic data and information. Confidential information is any patient information which includes but is not limited to medical records and is also any other non-public information or materials describing or relating to computer software or systems, business and financial affairs, employee information and personnel matters, operating procedures, organizational responsibilities, marketing matters, and policies and procedures of the Hospital Center or its employees, or other third parties.

1. All authorized users of the Hospital Center's computer equipment will have one or more unique user identifiers ("Passwords") which should not be shared with others. Passwords must be changed regularly, and no less than once every forty-five (45) days. Passwords shall be allocated to provide access to the Hospital's information in a way that is focused on the employee's specific responsibilities.

2. Employees should log off computers when away from their desks. Disks with confidential information should be kept in a secure place. In addition, disks should not be left where they can be exposed to magnets or where beverages or other liquids can spill on them.

3. Employees should immediately report to the IS Help Desk any suspected unauthorized access to patient information.

4. Employees should not take any steps which may expose the Hospital's computer resources to software viruses or other disabling devices. Employees may not accept, use or share programs or data from unauthorized sources.

VIOLATION OF POLICY

Violation of this Policy is grounds for disciplinary action up to and including termination. Unauthorized use of the Hospital Center's computer and communication systems may also subject employees to civil liability or criminal penalties.

Corp. Vice President for Human Resources _____

**ACKNOWLEDGMENT OF COMPUTER AND COMMUNICATIONS
SECURITY POLICY**

I have read _____'s [Hospital name] Computer and
Communications Security Policy in its entirety. I understand the policy and I agree to
abide by its terms.

Name (please print)

Signature

Date

