

COMPANY

Computer System Policies & Procedures

PURPOSE

This policy outlines accepted COMPANY practices and requirements for use of COMPANY computer systems, including Internet use and electronic mail. This policy is applicable to all related affiliates where services of COMPANY are being provided. This policy applies to all workers (management, staff members, physicians, contractors, consultants, volunteers, students, temporary staff members, etc.) who use the COMPANY computer systems.

COMPANY is responsible for securing its network and computer systems in a reasonable and economical manner against unauthorized access and/or abuse, while at the same time making them accessible to authorized and legitimate COMPANY users. This responsibility includes informing users of expected standards of conduct, and the consequences for not adhering to them.

INTERNET POLICY

The Internet is a powerful knowledge tool available to authorized COMPANY staff members through designated COMPANY computers. Although it is COMPANY's policy to use enhanced technology to ensure COMPANY network protection, the Internet is not completely reliable, nor is it a secure vehicle for transferring information or data, or for conducting electronic business.

Because of these factors, no confidential or patient care-related data are to be transferred to/from another Internet site, entity, or entity representative via the Internet, unless the data transmission is in total compliance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. This includes the transfer of this data via e-mail message and/or attachment capability provided through the COMPANY e-mail system or any other Internet e-mail service. Questions on HIPAA compliance and applicable regulations should be directed to the COMPANY Compliance Officer.

Any external Internet projects must be approved by the Vice President, Compliance Officer or Director of Communications. Approval is based primarily upon technical considerations, resource issues and compliance with HIPAA and other state and federal legislation.

Internet access, file downloads/uploads, file transfers and e-mail service via COMPANY resources are to be used for job-related functions. Internet access/use through COMPANY resources should not harm the image of the organization nor violate existing international, federal or state laws. Internet/World Wide Web accesses and sites visited may be monitored for appropriateness and effective use of COMPANY resources. Any instances of alleged abuse should be reported directly to the Compliance Officer. Improper use of Internet access as detailed in this policy is grounds for possible disciplinary action including suspension and termination of employment.

COMPANY

Computer System Policies & Procedures

INTERNET PROCEDURE

1. Ownership of Internet-Related Systems

Internet-related systems (including but not limited to computer equipment, software and operating systems, network accounts providing e-mail, World Wide Web browsing, File Transfer Protocol, networking and intranets systems and software) are the property of COMPANY. They are to be used for business services in serving the interests of COMPANY, our patients and our clients.

2. Network Security

COMPANY staff must adhere to all stated policies regarding network security. Each user must have a logon password and must not disclose his/her password to anyone other than the designated Network Administrator. It is advisable for staff to log off the system if they will be away from their computer for more than a few minutes.

3. Internet Access

Authorized COMPANY staff can access the Internet via software installed on designated desktop computers within each center. Such access is intended for job-related purposes.

4. Antivirus Software

To help protect COMPANY desktop computers against computer-related viruses, antivirus software is installed on COMPANY servers. Nonetheless it is advisable to refrain from opening e-mail messages and/or attachments from unknown sources.

5. File and Software Downloads

Internet sites may provide files and software that can be downloaded to an COMPANY computer. File downloads are restricted to approved job-related functions and should be undertaken only when essential. Downloads of software are entirely prohibited.

6. Visiting Web Sites

COMPANY's firewalls may prevent users from connecting with certain non-business web sites. Staff members using COMPANY computers should refrain from visiting web sites that contain sexually explicit, racist, violent or other potentially offensive material and must immediately disconnect from such a web site should such a connection accidentally occur. The ability to connect with a

COMPANY

Computer System Policies & Procedures

specific web site does not in itself imply that users of COMPANY systems are permitted to visit that site.

7. Resource Misuse

The following activities are prohibited:

- a. Unauthorized attempts to circumvent network security or exploit security vulnerabilities or decrypt secure data of COMPANY or any other individual, corporation or entity (hacking)
- b. Unauthorized attempts to monitor, read, copy, change, delete or tamper with another employee's electronic communications, files or software without the express approval of the user
- c. Knowingly or recklessly installing, running or distributing a worm, virus, Trojan horse or other harmful computer programs that could damage or place an excessive load on the COMPANY computer system
- d. Sending or making copies of documents, files, photographs, etc. in violation of copyrights held by individuals, corporations or other entities
- e. Attempted vandalism to the COMPANY network, computer equipment or software

COMPANY

Computer System Policies & Procedures

ELECTRONIC MAIL POLICY

COMPANY provides an electronic mail (e-mail) system for approved use by authorized staff members and approved third parties to simplify and expedite business-related communication. All information transmitted by e-mail will be treated as all other COMPANY records and become COMPANY property. COMPANY reserves the right to audit e-mail usage and/or to enter a staff member's e-mail files to audit messages sent over the COMPANY e-mail system.

COMPANY implements appropriate security procedures to prevent improper access to and disclosure of e-mail messages by unauthorized parties. Improper use of the e-mail system as detailed in this policy is grounds for possible disciplinary action including suspension and termination of employment.

ELECTRONIC MAIL PROCEDURE

1. System Conduct

- a. COMPANY e-mail users should use appropriate electronic etiquette, including but not limited to the following:
 - If you are sending your mail to multiple people and require a response from only one, address the mail to that one person and CC everyone else.
 - CC other additional parties only when necessary.
 - If you receive an e-mail, and you are designated as "To," you should respond as soon as possible, always within 24 workday hours.
 - Avoid using all capital letters, which is the electronic equivalent of shouting.
 - To maximize the efficiency of e-mail, keep the body of your message as brief as possible.
 - Be clear about the response you want and when you want it.
 - Re-read and spell check your message before you send it to ensure the information and tone are as you intended.
- b. COMPANY e-mail users must refrain from using harassing, threatening, offensive, obscene, demeaning, insulting, defaming, intimidating or sexually suggestive comments in e-mail messages. If any such violations occur:
 - Recipients should immediately print a hard copy of the inappropriate e-mail and give to their supervisors.

COMPANY

Computer System Policies & Procedures

- Supervisors should immediately and personally forward inappropriate printed e-mail messages given to them by their staff to the Vice President, the Compliance Officer and the Director of Communications.

2. Privacy of Communications

- a. While COMPANY desires to provide a reasonable level of privacy for COMPANY e-mail users, communications via e-mail are not private.
- b. COMPANY e-mail users should be aware that the data they create on the COMPANY system remains the property of COMPANY, and usually can be recovered even though deleted by the user.

3. Confidential Information

- a. Because e-mail transmissions are the property of COMPANY, confidential information (including but not limited to patient, employee, or financial information) should be transmitted via e-mail to any person outside COMPANY only when absolutely essential.
- b. Patient information may be transmitted to appropriate parties via e-mail only when it is done in total compliance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations.
- c. When using a distribution list to send confidential messages, always verify that the distribution list being used does not contain an inappropriate external e-mail address.

4. Security

- a. COMPANY implements appropriate security measures to prevent unauthorized access to e-mail files. Internal e-mail messages (those sent within the COMPANY e-mail system) cannot be accessed other than with sender's or recipient's expressed permission, except by an authorized Systems Administrator acting on instructions of COMPANY.
- b. COMPANY e-mail users must adhere to all stated policies regarding security and maintaining the confidentiality of passwords. Each e-mail user must have a logon password and must not disclose his/her password to anyone other than the designated Network Administrator.
- c. Passwords should be changed at least every six months to ensure proper security.
- d. COMPANY directors will regularly remind staff not to share e-mail accounts or passwords and to change passwords as indicated above.

COMPANY

Computer System Policies & Procedures

5. Personal Use

- a. Incidental and occasional personal use of e-mail is permitted within COMPANY, but such messages are subject to the same policies as other messages. Excessive or abusive personal use of the e-mail system is not permitted.
- b. Unless it involves an organization-approved activity (United Way, foundation-sponsored events, etc.), the COMPANY e-mail system must not be used for soliciting others for non-work purposes such as commercial, religious, charitable, political and personal causes or outside organizations.
- c. The sending of unsolicited junk mail, “for profit” messages, solicitations, promotions or chain letters through the COMPANY e-mail system is prohibited.
- d. It should be clear that personal e-mail messages are not official communications of COMPANY.

6. System Monitoring

- a. System Administrators and Internal Auditors may monitor business and personal e-mail communications for any breach in security, violation of law or infringement of COMPANY policy.
- b. If indications of illegal activity or violation of policy or security are found, incidences will be reported immediately to the Vice President, the Compliance Officer and the Director of Communications as appropriate.
- c. COMPANY e-mail users who engage in unauthorized use or violation of policy are subject to disciplinary action, including possible suspension or termination of employment.

7. COMPANY Access

- a. Appropriate officers and management of COMPANY may spot check and access and disclose the content of e-mail messages sent or received by COMPANY e-mail users whenever COMPANY considers it in its best interest, consistent with applicable law.
- b. Situations requiring access may include, but are not limited to, investigation of a potential breach of security of the electronic mail system, subpoenas, court order and other legal obligations of COMPANY and circumstances where COMPANY reasonably suspects a user is engaged in potentially unlawful activity or conduct that violates COMPANY policy.

COMPANY

Computer System Policies & Procedures

8. Distribution Lists

- a. COMPANY e-mail users must use distribution lists (public and private) carefully and with discretion, ensuring that the message is applicable to each individual on the list. When a message is not applicable to every person on the list, the message must be addressed individually to avoid non-relevant mail in COMPANY mailboxes.
- b. Staff members who are responsible for construction of public distribution lists must update their lists regularly to reflect changes in responsibility or employment status. Public distribution lists, as a whole, are maintained by the Director of Communications. Send all changes to communications@e-mailaddress.com.

9. Sending and Managing E-mail Attachments

- a. E-mail and file attachment storage space is limited. Individual users are responsible for ensuring that system space allocations are not exceeded and for managing it as listed below.
 - When possible, paste the document text into the body of the e-mail rather than attaching a file.
 - Only send a file attachment when the recipient(s) must have the file.
 - Save e-mail messages and file attachments only when needed.
 - Empty the deleted items folder regularly.

10. Receiving External E-mail Messages and Attachments

- a. All e-mail messages and attached files received from external e-mail systems (via the Internet) are automatically virus checked by the e-mail firewall as they are received at COMPANY. When a virus is detected, either within the message or within the attached file, the message and attachment are deleted and not distributed to the COMPANY recipient.

11. Third Party Use

- a. The COMPANY e-mail system may be used by COMPANY management, staff, physicians, individuals with COMPANY affiliates and entities and other third parties under certain management-approved circumstances. Third parties must abide by all established e-mail policies and procedures.

COMPANY

Computer System Policies & Procedures

PROCUREMENT OF COMPUTER HARDWARE AND SOFTWARE

All purchases of computer hardware and software for COMPANY must be approved by the Information Technology Group. Requests for purchase of hardware and/or software must be made in writing to the Information Technology Group. Under no circumstances should any unauthorized software be installed on any COMPANY server or computer.

REQUESTING TECHNICAL ASSISTANCE

When problems arise with the COMPANY computer system, technical assistance may be requested in the following manner.

1. If an emergency arises that affects the day-to-day business of COMPANY, immediately contact Information Technology Department at XXX-XXX-XXXX. An IT representative will respond to your request within 24 hours.
2. When technical assistance issues arise that do not require immediate attention, they should be submitted online by going to www.xxxxxxx.com. There you will be able to submit your problem and request technical assistance. An IT representative will respond to your request within 48 hours.

COMPANY
Computer System Policies & Procedures

Please return a completed copy of this form to your supervisor or directly to the Director of Human Resources. Everyone who has access to the COMPANY computer system is required to complete and sign this form.

I hereby acknowledge that I have read, understand, and will comply with the Company policies described above, and that I have been provided with a copy of these policies for my personal use. I understand a violation of these policies may result in disciplinary action, including possible termination and/or legal action.

Signature: _____

Print Name: _____

Date: _____