YOUR AGENCY EMS

Computer, Software, Network, and Internet Policy with Appropriateness of Use Guidelines

Date of Revision: January 2000
Date of Issue: February 2000

Approval Authority:

Issued under the authority of the Director of YOUR AGENCY Emergency Medical Services

Inquiries:

The Director of YOUR AGENCY Emergency Medical Services, or the system administrative staff

Application:

Personnel of the YOUR AGENCY Emergency Medical Services, to include full-time, part-time, relief, office, intern, and student personnel

Policy statement:

YOUR AGENCY EMS sponsored Internet/Intranet connections shall be used only by authorized users, for legitimate EMS business-related purposes and professional development

Policy requirements:

This policy concerns all connections to the Internet/Intranet made on behalf of YOUR AGENCY EMS. The YOUR AGENCY EMS Internet/Intranet and facilities are for official YOUR AGENCY EMS uses only. Use of the YOUR AGENCY EMS Internet/Intranet is restricted to activities that legitimately further the operations and programs of the department, including professional development

Supervision of users:

The Director, ALS Coordinator, and EMS Educational Coordinator should be aware of their subordinates' Internet/Intranet usage. Managerial accountability for the actions of subordinates applies equally to Internet use as to any other activity

Compliance with existing Acts and policies:

Information sent, received or published via the YOUR AGENCY EMS Internet/Intranet, and the circumstances under which it is accomplished, are subject to the same Acts and policies, listed herein under Source References, as

any other YOUR AGENCY EMS held information. In the event of disagreement with this policy, those Acts and policies shall prevail

Issues:

- YOUR AGENCY EMS Internet/Intranet consists of all facilities used by YOUR AGENCY EMS to connect to the local area network (LAN), the wide area network (WAN), and the global Internet

- Use of the Internet/Intranet on behalf of YOUR AGENCY EMS implies moral and ethical obligations

- Use of the Internet /Intranet to conduct departmental business is a leadership/chain of command issue

- The Internet/Intranet is an essential tool of day-to-day operations, and as such, must be properly utilized in order to provide value

- The unregulated nature of the Internet leads to a potential for waste of staff time and abuse

Privacy and monitoring:

There is no guarantee of privacy in using the Internet/Intranet, including e-mail communication. YOUR AGENCY EMS reserves the right to monitor all user Internet/Intranet communications and examine all information collected, created and/or generated as a result of using YOUR AGENCY EMS Internet/Intranet including any files, messages, printouts, removable media, or other material in order to monitor users' compliance with this policy

Integrity of information:

Internet/Intranet communication shall not be used for any official committal, contractual, or financial transaction involving YOUR AGENCY EMS, except within scope of authority

Ethics:

All users shall behave in a proper, ethical, and legal manner consistent with YOUR AGENCY EMS standards when they use the Internet/Intranet as they are entering into a public forum and any actions taken will reflect on the YOUR AGENCY EMS as a whole

Prohibited Activities:

Users of YOUR AGENCY EMS Internet shall not engage in prohibited activities as detailed in Appendix A

Expressing views:

Users shall avoid representing their personal views as being those of the YOUR AGENCY EMS or YOUR AGENCY government as users are not authorized spokespersons for either agency

Disciplinary actions:

Failure to comply with this policy and procedure may result in any or all of the following actions being taken:

- denying access to the YOUR AGENCY EMS Internet/Intranet and revoking of authorized user status
- payment of compensation for the misuse of resources
- departmental disciplinary procedure up to and including termination of employment
- prosecution according to law

Appendix A

PROCEDURES COVERING INTERNET/INTRANET USAGE

Definitions:

- **Netiquette** is a form of etiquette practiced within the Internet/Intranet environment

- **Authorized users** are individuals who have completed a Computer-Network Authorization Request form and been approved for an active account

Comment: I would remove the connection section…I've done so here

User Accounts:

- User accounts are assigned to individuals

- Users shall not share their accounts

- Users shall have full responsibility for the use of their account and will be held responsible for any policy violations that are traced to their account

User Passwords:

- Users shall read and comply with the Password Selection Guidelines

- Users shall access resources through the Internet/Intranet by using only those users IDs or methods that they have been authorized to use. Users shall not impersonate another person, use pseudonyms or be anonymous when communicating via the YOUR AGENCY EMS Internet/Intranet

- Users shall not share their passwords, or record their passwords on hard disk drives, e. g. within Web browsers or mail programs, or in any other insecure location. Failure to comply may result in disciplinary action

Netiquette:

- Users should familiarize themselves with the subject of network etiquette, customs and courtesies

- Users should familiarize themselves with the contents of all user guide material provided with respect to the system to which they are granted access, whether YOUR AGENCY EMS owned or external

- Users should release temporary connections to the Internet, such as dial-in connections, when not in use so as not to tie up modems and interfere with access by other users or support personnel

Prohibited Activities:

Users shall not engage in the following activities:

- **illegal use** of the YOUR AGENCY EMS Internet/Intranet for any purposes which violate applicable laws, including, but not limited to:

    - disseminating, mailing, posting, receiving or solicitation for the reception of illegal material such as child pornography, obscene, threatening, intimidating or harassing material, or hate propaganda, in any form; making public to YOUR AGENCY EMS or other users any such materials or direct links to such locations elsewhere on the Internet

    - use of the YOUR AGENCY EMS Internet to libel or slander other users, individuals or institutions

    - posting or in any way compromising the personal information of others as prohibited by the Privacy Act; to include Medic-Trak, Ticket-Trak and any other proprietary software

    - extortion

    - violation of copyright, trade secrets or infringement of any patent or other proprietary interest, including any activity that supports illegal distribution of software, otherwise known as pirating

    - gaining or attempting to gain unauthorized access to any kind of network, service, information, communications, or computing facility or resource through use of the YOUR AGENCY EMS Internet/Intranet

    - damaging/destroying the integrity of a computer system, or the data or programs stored on a computer system

- **personal use** of the YOUR AGENCY EMS Internet/Intranet:

    - for private purposes or for purposes not in the direct interests of YOUR AGENCY EMS (personnel with computers assigned to them may use the computer, web browser, and e-mail software for personal use provided that the rules for appropriateness of use are adhered to)

    - for displaying, receiving or disseminating sexual or pornographic material, in any form, for personal or non-work-related use, regardless of the legality of the material

    - for posting ads for money making schemes, including pyramid schemes

- **attempting to disable or circumvent security** mechanisms or access restrictions, or uncover security loopholes, or circumvent information/data protection schemes in order to gain unauthorized access;

- **disrupting service** by using the YOUR AGENCY EMS Internet/Intranet so as to interfere with or disrupt network resources, users, services or equipment. Examples of these include but are not limited to:

    - propagation of computer viruses, "worms", "Trojan horses" or other malicious code, including Virtual Viruses

    - maliciously physically disabling a computer or computer components

    - sending electronic chain letters or wide distribution e-mail

    - wasting resources (human, network capacity, computer)

    - making large numbers of article posts to inappropriate newsgroups (referred to as spamming)

    - playing network based games

- **attempting to monitor or tamper with** another user's electronic communications, except for monitoring by security and systems administrators in the performance of their authorized duties;

- **unauthorized**

    - publishing or distribution of official information; uploading, downloading, modifying, or removing files on any node in the network

    - posting files or information to the World Wide Web, newsgroups, or ftp servers without authorization

- **distributing or displaying material** which is in any way inconsistent with YOUR AGENCY EMS standards, community standards, or solicitation or reception of such material

- **contacting** software vendors, outside service vendors, outside network vendors, or any entity providing services or support to the YOUR AGENCY EMS computer and network system without express authorization of the Director

Users should be aware that the transfer of certain kinds of materials is illegal and a felony offense punishable by fine or jail sentence in the United States and elsewhere. Users should expect that evidence of such incidents would immediately be turned over to law enforcement authorities.

Users with an assigned computer need to receive authorization from the system administrative staff prior to taking their computer out of the United States. Some of the proprietary EMS software uses encryption technology that can't be legally removed from the United States. Request authorization even if traveling to Canada or Mexico. Violation of this can be punishable under the United States Felony Espionage and Munitions Control Laws that include mandatory jail sentences and very large fines.

If any computer or harddrive from a computer is lost or stolen, or you believe data has been removed from a computer without authorization, report it immediately so that proper authorities can be notified. Remember, we are managing legal records, private medical records, and we are using special encryption software to help maintain the security of these records. Information espionage is always a concern and users need to be vigilant to help protect the systems and data.

Appendix B

PASSWORD SELECTION GUIDELINE

The following password selection guidelines shall be observed:
The password must:

- be a minimum 6 characters in length
- be different from any other password used on any other YOUR AGENCY computer system
- not be a modified login name in any form (as-is, reversed, capitalized, doubled, etc.)
- not be the user's first, middle or last name in any form
- not be the user's spouse's or child's name
- not be other information easily obtained about the user. This includes but is not limited to: license plate numbers, telephone numbers, the make of an automobile, the name of the street, etc…
- not contain all digits, or all the same letter
- not be a word contained in English, French, Spanish, German, Dutch, Chinese, Japanese or Russian or any foreign language dictionaries, spelling lists, or other lists of words

Methods of selecting a password, which adheres to these guidelines, include:

- choosing a line or two from a song or poem, and use the first letter of each word
- alternating between one consonant and one or two vowels, up to at least seven characters. This provides nonsense words which are usually pronounceable, and thus easily remembered
- choosing two short words and concatenating them together with a punctuation character between them
- choosing random alphanumeric characters (numbers and both upper and lower case letters)

Appendix C

INTERNET/INTRANET SECURITY

Virus Protection:

In order to prevent spreading viruses to the Internet or YOUR AGENCY EMS owned facilities, users shall scan for viruses and other malicious code:

- when any diskette or other storage medium is transferred from an Internet connected workstation to a YOUR AGENCY EMS workstation
- upon downloading files from the Internet, particularly executable programs and other files at risk such as documents containing macros, and applications which may be downloaded and executed automatically such as JAVA applets
- before uploading any files to the Internet
- upon receiving or sending Internet e-mail attachments
- when using a privately owned workstation to connect to YOUR AGENCY EMS Internet

Information Security:

- Internet communication is considered to be totally unsecured unless encrypted and digitally signed
- Users shall report any inappropriate or illegal material they find on a YOUR AGENCY EMS Internet site to the Director, ALS Coordinator, EMS Education Coordinator, or System Administrative staff for investigation
- Users are responsible for knowing whether or not release of information or opinions could constitute a security breach or result in an embarrassing situation

System Security:

If a user finds that they are able to circumvent system security, the user shall inform the Director, ALS Coordinator, EMS Education Coordinator, or System Administrative staff in order that steps can be taken to prevent further occurrences