SECTION - HOSPITAL OPERATIONS
ADMINISTRATIVE DIRECTIVE NO. 746
(Replaces AD 746 dated 1/19/06)

Effective Date: December 7, 2006

SUBJECT: INTERNET ACCESS AND E-MAIL USE

I. PURPOSE

A. The purpose of the Coalinga State Hospital (CSH) Internet Access and E-mail Use Policy is:

1. To define facility policy and procedures for accessing the Internet.

2. To establish use of the Internet and E-mail as an appropriate means of communication for both information access and information dissemination by staff.

3. To encourage the productive use of the Internet and E-mail by employees as a mechanism to accomplish departmental goals.

4. To establish consistent standards and guidelines to ensure that the use of the Internet and E-mail is efficient, cost effective, and minimize risk to facility computer systems, electronic data and confidential files.

5. To establish necessary Internet and E-mail support functions within the facility.

6. To comply with the data security requirements of the State Information Technology Security and Risk Assessment Policy (State Administrative Manual Sections 4840-4845).

B. This Internet Access and E-mail Use Policy provide facility employees with guidelines for accessing and disseminating information via the Internet and E-mail. The policy:

1. Describes the Internet and identifies a structure for its use.

2. Establishes infrastructure for Internet access and E-mail use.

3. Recognizes that the Internet and E-mail can benefit the facility and its customers.

4. Provides guidelines on using the Internet and E-mail to improve services and enhance productivity.

5. Minimizes the risks of using the Internet and E-mail.

II. AUTHORITY

Department of Mental Health, Special Order Number 510, consistent with the authority provided in Government Code Section 11152 establishes the required authority for this directive.

By the order of the Hospital Executive Director or his designee will be responsible for determining what information will be provided through facility Internet and E-mail services. All public information to be placed on the Internet, regardless of the source, will be cleared in accordance with public information release policies and procedures.

III. POLICY

This policy applies to all Internet and E-mail activities in the facility. All employees must adhere to the following procedures:

A. Internet and E-mail access utilizing facility resources on state time is solely for the purpose of conducting state business.

B. All Internet and E-mail activities may be monitored by the Information Technology (IT) Department.

C. Employees needing Internet or E-mail access may submit a "Request for Internet Access" Form (MH 3271) to their Department or Program Director.

D. Upon the Department or Program Director's preliminary recommendation for approval, the request will be forwarded to the Information Technology Department.

E. Supervisors are responsible for monitoring their employees' Internet and E-mail activities to ensure compliance with this policy.

F. Individuals using hospital equipment to access the Internet and E-mail are subject to having activities monitored by system or security personnel. Use of this system constitutes consent to security monitoring.

IV. METHOD

The IT Department shall support the Internet and E-mail functions within the facility. IT shall obtain guidance on the implementation of Internet access and E-mail use from the facility administration and Information Management Committee. IT and the Information Management Committee shall be responsible for:

A. Providing direction for the use of the Internet and E-mail including, but not limited to, formalized training.

B. Reviewing and updating Internet and E-mail policy standards and procedures.

C. Internet and E-mail planning and oversight to ensure application and implementation strategies are consistent, efficient and cost-effective.

D. Ensure that all personal computers with Internet and E-mail access will utilize an anti-virus program that is installed and updated regularly by the IT Department.

E. Developing and implementing an Information Technology Security Awareness and Training Program for all hospital employees and contractors working with sensitive information systems. This program will cover initial training for new hires/transfers, continuing efforts to create heightened security awareness, and regular refresher training.

F. Ensuring that:

1. Requests for access can be honored based on the configuration or location of the individual system.

2. Additional resources necessary to implement access are available.

3. Employees receiving approval attend in-house Internet and E-mail training.

4. Software is properly installed.

5. Access is initiated and revoked as appropriate.

6. Access is strictly limited to those employees who have been formally approved.

V. RESPONSIBILITIES

A. Supervisor Responsibility:

Supervisors of hospital employees, volunteers, and contractors will have the final authority in determining appropriate versus inappropriate Internet and E-mail behavior. Supervisors have the responsibility for acquiring Internet and E-mail access for their employees who need it.

B. Employee Responsibility:

1. Information Content and Use of the System – Acceptable Uses:

The state reserves the right to monitor and/or log all network activity with or without notice, including E-mail and all web site communications; and therefore, users should have no reasonable expectation of privacy in the use of these resources.

2. Uses that are Acceptable and Encouraged:

a. Communications and information exchanges directly relating to the mission, charter, and work tasks of the agency;

b. Announcements of state laws, procedures, hearing, policies, services, or activities;

c. Use for advisory, standards, research, analysis, and professional society or development activities related to the user's state governmental duties;

d. Use in applying for or administering grants or contracts for state government research programs.

3. Uses that are Unacceptable:

a. It is unacceptable for a user to use, submit, publish, display, or transmit on the network or on any computer system any information that:

i. Violates or infringes on the rights of any other person, including the right to privacy;

ii. Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;

iii. Violates agency or departmental regulations prohibiting sexual harassment;

iv. Restricts or inhibits other users from using the system or the efficiency of the computer system;

v. Encourages the use of controlled substances, or uses the system for the purpose of criminal intent;

vi. Uses the system for any other illegal purpose.

b. It is also unacceptable for a user to use the facilities and capabilities of the system to:

i. Conduct any non-approved business;

ii. Solicit the performance of any activity that is prohibited by law;

iii. Transmit material, information, or software in violation of any local, state, or federal law;

iv. Conduct any political activity;

v. Conduct any non-governmental-related activities;

vi. Engage in any activity for personal gain or personal business transactions;

vii. Make any unauthorized purchases;

viii. Make any connections to "streaming video/audio" unless pre-approved by the Director of Information Technology;

ix. Engage in any "instant messenger" communication unless pre-approved by the Director of Information Technology.

4. Etiquette and proper use of distribution lists:

a. Users with Internet and E-mail access are expected to maintain proper etiquette and professionalism within all communications.

b. System wide distribution lists (All_CSH) should be used only for appropriate work related issues and must be approved by the Department manager or Program Director prior to distribution.

5. Archiving and maintenance of E-mail system:

All users will be provided with an offline archive location for storage of critical historical mail messages. Users are encouraged to perform regular archiving and mailbox cleanup to ensure the most efficient use of mail system resources. Unnecessary messages should be deleted on a regular basis and not archived.

6. Copyrighted Material:

   Users may download copyrighted material, but its use must be strictly within the agreement as posted by the author or current copyright law. The Federal Copyright Act at 17 U.S.C. 101 et. seg. (1988), protects and prohibits misuse of all original works of authorship in any tangible medium of expression. This includes a prohibition on plagiarism (using someone else's ideas or writing and passing it on as one's own).

7. Public Domain Material:

   Any user may download public domain programs for his/her own business-related use, or may redistribute a public domain program non-commercially, but does so with the knowledge that by doing so he/she also assumes all of the risks regarding the determination of whether or not a program is in the public domain.

8. Electronic Mail (E-Mail):

   E-mail is considered network activity, thus, it is subject to all policies regarding acceptable or unacceptable uses of the Internet, and the user should not consider E-mail to be either private or secure.

VI. PRESENTATION OF INFORMATION

CSH shall take advantage of current technology to serve as wide a customer base as possible. Confidential information will not be transmitted via the Internet. E-mail across the Internet shall not contain confidential information.

VII. IMPLEMENTATION AND REVIEW

Implementation of this directive is the responsibility of the Information Management Committee.

W. T. VOSS
Executive Director

Cross Reference:
A.D. No. 742 - Hospital Computers