SECTION - HOSPITAL OPERATIONS
ADMINISTRATIVE DIRECTIVE NO. 742
(Replaces AD 742 dated 9/15/2005)

Effective Date: August 10, 2006

SUBJECT: HOSPITAL COMPUTERS

I. PURPOSE

The use of the word "Personal Computer" in this document means any desktop, lap top, palm held computer or other electronic equipment that is capable of entering, storing and reporting information.

The purpose of this policy is to establish standards for the use and management of personal computers within Coalinga State Hospital (CSH). The policy recognizes the potential for increasing employee productivity through the appropriate use of personal computers and is intended to promote such use.

II. AUTHORITY

Section 4989 of the State Administrative Manual (SAM) limits the personal computer policy to single-user desktop, and portable computers used to increase the productivity of individual employees. Applications involving networking of personal computers or communication with mainframe computers is not excluded from this policy, except as specified in Section 4989.1 of the SAM.

Administrative units wishing to initiate information technology projects that do not fall under the personal computer policy must follow the procedures for planning and justifying such projects specified in Section 4819.3 of the SAM.

III. POLICY

Use of state owned computer equipment, including Personal Computers and associated peripherals is subject to the following provisions:

A. Personal and non-state business use is prohibited.

B. Software development on facility Personal Computers is to be reviewed and approved by the area manager and the Data Processing Manager prior to the initiation of development.

C. All equipment is regarded as a hospital asset and not "owned" by a specific program/department. Assignment/reassignment of the equipment is based on the analysis of needs.

D. Software not owned and procured by the state is not to be placed on any state-owned computer system. All software obtained as the result of a donation/gift to the hospital will be reviewed for licensing, compatibility, technical support and functionality by Information Technology. The Data Processing Manager will make a determination whether to accept or reject the donation/gift.

E. Hardware not owned and procured by the state is not to be attached/connected to any state owned computer system. All hardware obtained as the result of a donation/gift to the hospital will be reviewed for compatibility, support and maintenance cost by Information Technology. The Data Processing Manager will make a determination whether to accept or reject the donation/gift.

F. Software owned by the state is not to be duplicated in any form, except as outlined under the provisions of the software publisher/manufacturer. Proprietary software is protected under the Federal Copyright Law. It is illegal to make or distribute copies of software, except to make a backup copy for archive purposes (only). Modification and or duplication of software for any other reason, including for sale, loan, rental or gift, is a federal crime. Penalties include fines of as much as $50,000 and jail terms of up to five (5) years.

G. Information Technology Staff will conduct and record random spot inspections of facility Personal Computers. Discrepancies of any nature (including software/hardware not owned by the state) will be documented and reported to the Executive Director, including recommendations for correction.

IV. METHOD

A. Approval of Equipment and Software: Administrative units proposing to acquire personal computer(s), associated personal computer equipment and/or personal computer software are expected to confer with the Data Processing Manager. Information Technology Staff have information on items to be selected that meet specifications, are appropriately priced, and are compatible with systems already in use in CSH, the Department of Mental Health, or in other state agencies. Minimum standards will continuously be updated in response to changing technology.

B. Development of Software for Personal Computers: It is the policy of CSH to use commercial software packages for personal computers whenever possible, rather than undertake independent software development. Fully tested and documented commercial packages are readily available for most personal computer functions and are usually much less costly than custom-developed programs. In addition, applications development by state employees or contractors does NOT fall within the personal computer policy and must be justified in accordance with the requirements for an information technology project (SAM Section 4891.3).

C. Approval of Acquisition: Each request for acquisition of a personal computer system, associated equipment, software, or computer related training is subject to management review and approval before the order can be placed or the

program/department takes possession of any computer equipment or software. The Personal Computer justification must be submitted using Information Technology Request Form (GA 545IT) which provides for necessary approval signatures and certifications. These forms are available in your Information Technology Department.

D. Procedure for Acquisition: Program/Department management is responsible for preparing the needs assessment and justification associated with the proposed acquisition of a personal computer, personal computer software, or associated equipment. Normally this process will be documented using the Information Technology Request Form (GA545IT). In some cases, if the acquisition is unusually complex or is critical to the accomplishment of CSH's objectives, a Feasibility Study Report must be prepared in accordance with Sections 4921 through 4928 of the State Administrative Manual.

Once the need for a personal computer is documented and has been approved by Program/Department management, the Information Technology Department, in cooperation with Program/Department management, will prepare technical specifications and the appropriate procurement documents. A copy of this documentation will be maintained in Information Technology Department files.

E. Electronic Mail: Electronic mail shall be used to facilitate timely communication among employees within the Department and to streamline Department processes. Staff may use e-mail for work-related activities only. No confidential data shall be transmitted via e-mail outside of the Department of Mental Health. Information Technology Department may monitor e-mail activities and shall report any inappropriate correspondence to the Hospital Administrator. The use of Electronic Mail shall conform to the provisions of CSH Administrative Directive 746 – Internet Access and E-mail Use.

F. Security: The use of personal computers within CSH shall be in accordance with all applicable provisions of the State Administrative Manual dealing with information security and risk management (Section 4840 through 4845), the specific provisions of SAM Section 4989.7 dealing with personal computer security and DMH Special Orders 518 and 520. Security controls shall be implemented as follows:

1. Password Security

    a. User passwords are the property of each User and are not to be shared or recorded where they are recognizable or easily obtainable by other staff.

    b. The Information Technology Department will implement appropriate controls to ensure that computer system password requirements meet "strong" password criteria, including a minimum of eight (8) characters and characters from at least three (3) of the following categories – English uppercase characters, English lowercase letters, Numeric characters, Special characters.

c. Password changes will be forced every 90 days and three (3) unsuccessful login attempts will disable the user account. Passwords shall not be reused within a one year period.

d. Default passwords for vendor systems under local control will be changed prior to being placed into production.

e. Letting someone else use your password, or your network account after you have logged on is a security risk and violates confidentiality rules. The Information Technology Department may monitor network log-ins and shall report inappropriate activities to the Hospital Administrator.

2. Workstation Security

a. Workstations & monitor screens shall be positioned to prevent unauthorized visual access to confidential or sensitive electronic information. Privacy screens shall be used where physical limitations limit repositioning of equipment.

b. Workstations shall be physically protected against theft and/or unauthorized access according to the physical attributes of the surroundings.

c. Portable devices shall not be used to access, process, or store confidential or sensitive electronic information unless the information is encrypted and protected from theft and/or unauthorized access.

d. Workstations shall be logged off or locked when leaving workstation and logged off prior to leaving the facility.

e. Confidential or sensitive information shall be stored on network directories on networked workstations.

f. Confidential or sensitive information on standalone workstations shall be physically safeguarded against theft and/or unauthorized access.

g. Confidential and/or sensitive data maintained in a personal computer must be subjected to the same degree of management control as any other confidential and/or sensitive information.

G. Protection from Malicious Software (Viruses)

In Accordance with DMH Special Order 516, the Information Technology Department shall implement system wide controls to protect CSH information system assets from malicious software. Anti-virus client software will be installed on all computers and configured to maintain proper updates. All computers will have daily scheduled system scans and scan opened files in real time, including e-mail attachments.

Incidents of detected viruses shall immediately be reported to the Data Processing Manager. Infected workstations not able to be cleaned shall be removed from the network until cleaned or re-imaged by Information Technology staff.

H. System Backup: In accordance with DMH Special Order 515, provisions must be made to protect against the loss of data and programs stored in personal computers as a result of machine or power failures. The Information Technology Department shall keep original program software diskettes. Data owners will create copies of their data files on stand-alone computers. A regular schedule for making backup copies of all data files on stand-alone computers shall be established by the data owner. Program/Department management shall ensure that backup procedures are carried out. Information Technology staff will complete backups of the network data to offsite storage locations & perform regular system restores to validate backup files.

I. Documentation: The Information Technology Department is responsible to see that complete documentation and software licensing is maintained for each personal computer system. Documentation shall be kept and will include:

1. Hardware:

   a. Inventory. Inventory sheet of complete system, provided by Information Technology Department.

   b. Installation, Maintenance and Care. All documentation relating to the installation, maintenance, and care of the equipment.

   c. Hardware Manuals. Location of all hardware manuals that relate to the system.

2. Software:

   a. All software and software licenses will be installed, managed and stored by Information Technology Department. All software manuals relating to the installation and proprietary software shall be kept by Information Technology Department.

   b. Backup Diskettes. Program/Departments are responsible for backup schedule and location of all data backup diskettes for stand-alone computers.

3. Procedural Documentation: Each application that makes use of a proprietary software package (including database systems, spreadsheet systems, or any software that maintains data files) must have procedural documentation sufficient to allow productive use of the application in the absence of its primary user. This documentation will normally consist of the following:

a. user instructions documenting the scope and purpose of the applications;

b. specific data entry and processing instructions for the application;

c. detailed file descriptions including data dictionaries;

d. lists of all utility programs and subroutines used by the application; and:

e. sample report and screen formats for the application.

J. Training: Program/Department management is responsible for ensuring that staff members possess the knowledge and skills necessary for effective use of the personal computers that are available to the Program/Department. They are also responsible for ensuring that there is sufficient depth of staff training to prevent disruption of key activities in the event of unexpected staff changes.

K. Ergonomics: Program/Department management is responsible, within available resources, for providing ergonomically designed workstation equipment that is adjustable. In keeping with the Title 8 Regulation on Ergonomics and our goal to reduce injures associated with repetitive motions, all staff using computers must complete an ergonornic workstation evaluation with their supervisor using the "Computer User's Handbook." The Health and Safety Department should be contacted for details regarding the evaluation.

L. Maintenance and Repair: The hospital will make provision for necessary maintenance/repair of personal computers and related equipment. Problems with the operation of a personal computer should be reported to the Information Technology Department, who will create a work order for appropriate repair services.

M. Device & Media Controls. In accordance with DMH Special Order 523, the Information Security Liaison shall maintain a tracking document to monitor the receipt of hardware and/or electronic media containing confidential or sensitive information when it enters CSH. The hardware and/or media shall be labeled and scanned for viruses prior to being provided to workforce staff. Workforce staff shall create a tracking document to track the movement of confidential information between workforce members. This document shall include the Date & time of transfer, name of individual releasing the media, name of individual receiving the media and a description of contents. Media used to copy or transfer data within the facility does not require documentation provided that.

N. Remote Access: In accordance with DMH Special Order 517, remote access shall only be allowed based on demonstrated need and must be approved by the Information Security Liaison and meet all security provisions applicable to workstations located within the secure facility.

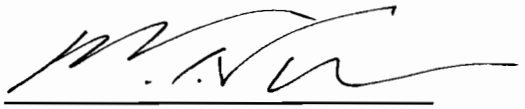
O. Information Security Liaison: In accordance with Special Order 521, Coalinga State Hospital will appoint an Information Security Liaison (ISL) to work closely with the DMH Information Security Officer (ISO) to ensure conformance with all provisions of the State Administrative Manual and the Health Insurance Portability and Accountability Act of 1996 Security Rule. The ISL for Coalinga State Hospital shall be the Data Processing Manager.

P. Information Security Incident Response: In accordance with Special Order 522, any suspected or actual information security incidents shall be immediately reported to the DMH Information Security Officer or to the hospital's Information Security Liaison for investigation and appropriate action.

V. RESPONSIBILITIES

A. Management Responsibility: Personal computers are considered hospital resources and management responsibility for the use of each personal computer, as well as the security of data, equipment, and software associated with the personal computer, is assigned to the manager who is responsible for supervising the personnel who regularly use the personal computer. The personal computer may be assigned for the exclusive use of any individual or unit within the hospital, but such assignment may be changed at any time.

B. Personal Computer Coordinator: Responsibility for the personal computer coordination and technical assistance has been assigned to the Data Processing Manager.



W. T. VOSS
Executive Director

Cross Reference(s)
A.D. No. 746 - Internet Access and E-mail Use
DMH Special Order 515 – Data Backup and Storage
DMH Special Order 516 – Protection from malicious Software (Viruses)
DMH Special Order 517 – Remote Access
DMH Special Order 518 – Workstation Use and Security
DMH Special Order 520 – Password Management
DMH Special Order 521 – Information Security Liaison
DMH Special Order 522 – Information Security Incident Response
DMH Special Order 523 – Device and Media Controls