

 <p>HAWAII HEALTH SYSTEMS C O R P O R A T I O N <i>"Touching Lives Everyday"</i></p> <p>Policies and Procedures</p>	Department: Information Technology Department	Policy No.: ITD 0001
	Issued by: Dennis Sato Vice President & CIO	Revision No.: N/A
Subject: PC Hardware and Software – Acquisition & Use	Approved by: Thomas M. Driskill, Jr. President & CEO	Effective Date: September 15, 2000
		Supersedes Policy: N/A
		Page: 1 of 6

I. PURPOSE: To establish and maintain guidelines for effective control over the acquisition and use of PC hardware and software systems within the Hawaii Health Systems Corporation (HHSC) and its facilities. To identify the type of PC hardware and software that will be supported and maintained by the Information Technology Department (ITD). To define PC-based application software that is to be used throughout HHSC and its facilities as the approved Corporate standard.

II. POLICY: The ITD will establish and maintain the operational guidelines for the acquisition of PC hardware and software. All hardware or software to be used within HHSC and its facilities will conform to these guidelines if it is to be connected to the HHSC local or wide-area network or to be used in conjunction with an application area that has been standardized by the ITD.

These guidelines will include the identification of the Corporate standards of select PC-based applications and usage including, but not limited to, word processors, presentation software, spreadsheets, Internet access, and internal and external e-mail systems.

This policy will be conducted in accordance with the respective collective bargaining agreements.

III. SCOPE: This policy applies to all HHSC employees and other authorized designated users of HHSC hardware and software.

IV. COMMENTS/OTHER REMARKS:

- A. See policies and procedures related to security and requests for access to systems (technical & applications).
- B. Suggestions or comments on this policy should be directed to the HHSC Chief Information Officer.
- C. Copies of this and other ITD policies and procedures are files in the HHSC Systems Manual.

V. PROCEDURE:

- A. **Configuration Guidelines:** All personal computer (PC) software and hardware, and other computer workstations acquired for use within HHSC and its facilities that are to be supported by the ITD will be configured in accordance with the following standard hardware and software configuration guidelines.
1. The Director of Technical Services will, at a minimum of once per calendar year, review and revise, if necessary, the HHSC standard hardware and software configuration specifications in order to ensure that the latest and most cost effective technology remains available to HHSC and its facilities. Standards are defined in the HHSC Systems Manual.
 2. Any proposed revisions to the standard specifications will be reviewed and approved by the HHSC Chief Information Officer and the Directors of Application Services, Technical Services and Regional End User Services. The process for request and approvals are listed in HHSC Systems Manual.
 3. PC hardware or other hardware devices to be connected to an HHSC local or wide-area network will be configured to conform to the specifications defined in the HHSC Systems Manual. Hardware for which no specifications have been defined must be reviewed and approved by the Director of Technical Services prior to its acquisition and connection to the network.
 4. The PC software for all standardized application areas will be selected from the list of approved software packages defined within the HHSC Systems Manual.
 5. PC software for application areas for which no HHSC standard has been identified must be reviewed by the ITD and approved in writing by the Director of Technical Services before it is loaded on to any PC or other device connected to an HHSC local or wide-area network. Nonstandard software applications will not be supported by the ITD unless the Director of Technical Services approves such support in writing. Signed authorizations will be maintained by ITD. (This includes, but is not limited to, screen savers, clipart, etc.) The System Request and Problem Report form will be used for this process (see IT Policy 8.000).
- B. **Hardware and Software Purchase Requests:** All hardware and software purchase requests for HHSC and its facilities must be reviewed by the Director of Technical Services to assure compliance with established standards and compatibility with existing systems. The Director of Technical Services will initial the purchase request to show concurrence. Materials Management and Financial Services Department procedures for these purchases also apply.
- C. **Program Backups:** ITD will provide backups of user programs and files stored on network file servers in accordance with its published back-up schedule. The schedule is located in the HHSC Systems Manual. ITD will assist users in the restoration of back-up programs or files as may be necessary. Individual users will be responsible for backing up programs and files stored on their PCs local disk drive. Help Desk assistance will be available to the users from the respective REST, ASD or TSD staff.
- D. **Security:** A PC offers little or no security for data stored on its local disk drive. Users will not store confidential or secured data on their PC unless physical access to the PC can be adequately controlled. Confidential data may also be stored on diskette provided such diskettes are stored in a secure or locked area.

1. The Director of Technical Services will assist users in assessing the adequacy of the physical security of their PC environment.
2. Confidential data will normally be stored on HHSC network file servers that are secured by user login restrictions.

E. E-mail:

1. Microsoft Exchange will be the approved standard for e-mail service for HHSC and all its facilities. The standard configuration information for e-mail service is defined within the HHSC Systems Manual.
2. Email users will follow the guidelines distributed when they are granted email access. Email guidelines include and are not limited to the following:
 - a. *Good Sender Habits:*
 - 1) *Use distribution lists with caution. Send e-mail messages only to recipients who need the information.*
 - 2) *Be succinct. The most effective e-mail messages are short and to the point.*
 - 3) *Keep the message focused on a single topic.*
 - 4) *Include a subject line that captures the content of the message. This helps recipients prioritize, file, and search for messages.*
 - 5) *Tag messages appropriately. Do not tag messages as "High Priority" or "Urgent" if they are not.*
 - 6) *Do not modify someone else's message.*
 - 7) *Do not broadcast someone else's message without permission.*
 - 8) *Do not "reply to all" unless they all need to see your reply.*
 - 9) *Do not originate or forward unsolicited e-mail (i.e., chain letters).*
 - 10) *Choose the number and size of file attachments with great care.*
 - 11) *Address e-mail according to the expected action. A person listed in the "To" field is expected to respond; one in the "CC" field is expected to read the message as information only.*
 - 12) *Avoid long dialogues and threads via e-mail. The duration of the thread, too many topics and too many people can lead to confusion.*
 - 13) *Consider message format. There is no guarantee that the user's e-mail client will display the message as intended by the sender. Do not depend on alignments, fonts or colors to make a point.*
 - b. *Good Recipient Habits*
 - 1) *Develop regular intervals for using e-mail.*
 - 2) *Delete messages that are no longer needed.*
 - 3) *File important messages into organized folders.*
 - 4) *Browse the subject line to identify important messages.*
 - 5) *Reply or acknowledge receipt of messages promptly if the originator is expecting a response.*
 - 6) *Use auto-replies or delegate authority when unable to check e-mail.*
 - 7) *Use inbox rules and filters to file messages automatically to relevant folders.*
 - 8) *Delete junk mail.*
 - 9) *Request to be removed from unwanted distribution lists.*
 - 10) *Do not reply to all recipients unless they all need to see your reply.*
3. The HHSC Mail Service is an effective and useful means of communication when properly used. The use of HHSC Mail is restricted to company business only as

necessary to carry out assigned duties. No personal or commercial messages are allowed.

4. Prohibited activities include, and are not limited to: sending, receiving, displaying, printing or otherwise disseminating material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating or defamatory is prohibited. Copyrighted materials may not be distributed through HHSC e-mail without appropriately documented permission.
5. Prohibited uses include, but are not limited to: employees may not use HHSC e-mail for commercial or personal advertisements, solicitation, promotions, destructive programs (i.e. viruses and/or self-replicating code), political material, or any other unauthorized or personal use.
6. HHSC Mail Service users should routinely monitor their mailbox to ensure effective use of disk space. Saved e-mail messages should be filed into private files, and the individual user should routinely delete old and unwanted e-mail.
7. The HHSC Mail System Administrator is authorized to establish and enforce resource limitations on individual user accounts to prohibit the excessive use of resources. The HHSC Mail System Administrator will perform periodic cleanup, and is authorized to delete older e-mail messages from individual mailboxes as may become necessary for proper resource management.
8. Prohibited uses should be reported to your supervisor, your facility's System Administrator, HHSC ITD or Human Resources Department.
9. Any violation of the above may result in loss of system privileges, disciplinary action, civil and/or criminal liabilities upon completion of a thorough investigation. Discipline will follow language provided in collective bargaining agreements and HHSC Personnel Policies and Procedures.

F. Internet Use:

The Internet is a worldwide network of computers containing millions of pages of information and many diverse points of view. Because of its global nature, users of the Internet may encounter material that is inappropriate, offensive, and in many instances, illegal. System users are responsible for the material they review and download on the Internet.

1. Users may only access the Internet through an approved Internet firewall.
2. Prohibited activities include, but are not limited to: sending, receiving, displaying, printing or otherwise disseminating material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating or defamatory is prohibited.
3. Prohibited uses include, but are not limited to: employees may not use HHSC Internet resources for commercial or personal advertisements, solicitations, promotions, destructive programs (i.e. viruses and/or self-replicating code), political material, or any other unauthorized or personal use.
4. Communicating Information. Employees will exercise the same care in communicating in chat groups and posting items to newsgroups as they would for any other written communication. Anything created on the computer or Internet may, and likely will, be reviewed by others.
5. Disclaimer of Liability. HHSC will not be responsible for any damages, direct or indirect, arising out of the use of its Internet resources. The HHSC System

Administrator is authorized to monitor Internet usage on the network including, but not limited to, monitoring sites employees visit on the Internet, monitoring chat groups and newsgroups, and reviewing material downloaded or uploaded by employees.

6. Compliance with Applicable Laws and Licenses. Employees must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property and online activity.
7. Prohibited uses should be reported immediately to your supervisor, your facility's System Administrator, HHSC ITD or Human Resources Department.
8. Any violation of the above may result in loss of system privileges, disciplinary action, civil and/or criminal liability upon completion of a thorough investigation. Discipline will follow language provided in collective bargaining agreements and HHSC Personnel Policies and Procedures.