

 <p>HAWAII HEALTH SYSTEMS C O R P O R A T I O N "Touching Lives Everyday"</p> <p>Policy</p>	Department: Information Technology Department	Policy No.: ITD 0019
	Issued by: Barbara Kahana Vice President & CIO	Revision No.: 2
Subject: Workstation (Computer) Use	Approved by: Thomas M. Driskill, Jr. President & CEO	Effective Date: 10/1/07
		Supersedes Policy: 10/04/04
		Page: 1 of 3

- I. **PURPOSE:** This policy defines appropriate standards for secure use of HHSC workstations by the HHSC workforce to protect the confidentiality and integrity of information in order to comply with State and Federal laws, including but not limited to, the Health Insurance Portability and Accountability Act (HIPAA).
- II. **POLICY:** The following provisions shall apply to HHSC workstations/devices:
- **WORKSTATION ADMINISTRATION**
 1. Workstations are the property of HHSC and are provided to the HHSC workforce for business use. Non-HHSC owned devices, such as but not limited to, Hubs, Access Points, Laptops, Handheld devices, are not permitted to be connected to the HHSC network. Exceptions shall be requested and be submitted for approval via the change management form.
 2. Only properly licensed, authorized software may be installed on HHSC workstations.
 3. The Technical Services Division (TSD), subject to ITD 0002 (Security Configuration Management Policy), shall determine HHSC software and hardware configuration standards in collaboration and approval from the Regional End-User Support Team (REST).
 4. Only authorized TSD or REST staff shall perform Software installation and hardware configuration modifications.
 5. Modems are prohibited from being connected to any HHSC workstation that is connected to the HHSC network. Users who require dial-out capability must use the HHSC secure modem bank.
 6. Dial-in access to workstations connected to HHSC's network by modem is prohibited. Remote access methods are described in ITD 0006 (Remote Access Policy).
 7. E-mail and Internet use are addressed by ITD 0017 (Electronic Mail Policy) and

ITD 0018 (Internet Use Policy), respectively.

8. Commercial Peer-to-peer (P2P) software is insecure and must not be installed on any workstation.
9. Anti-Virus software must not be disabled.
10. Workstations must be set to utilize some type of workstation inactivity timeouts that will lock the workstation, for example password protected "screen savers". The recommended timeout period is 15 minutes. Also, PC's that support multiple Users such as Nursing Stations may be excluded from workstation locking.
11. Streaming Audio and Video is resource intensive and therefore will only be used for business purposes. All other uses are prohibited.

• **WORKSTATION USE**

1. Workforce must position monitors so that unauthorized persons cannot easily see their display contents. If necessary, use a monitor privacy filter.
2. Workforce must not leave printers and fax machines unattended when they are printing/sending/receiving confidential patient/employee information. If printers and fax machines are in a general area the user will be diligent in picking up confidential reports in a timely manner.
3. Workforce may not store or save confidential information from HHSC's system onto diskette, CD, flash drive, portable device, or other removable media without the express permission of their supervisor with the understanding that such data will be encrypted, handled securely and disposed of properly.
4. Workforce will save documents and data containing confidential information on HHSC's file servers. There should be no confidential information stored on local hard drives or removable storage for example, laptop hard drive; USB drives etc. unless it is encrypted with approved software.
5. Workforce will not use USB storage devices. In an effort to prevent the unauthorized use of USB storage devices a system-wide setting will be implemented to disable USB ports. USB ports can be enabled with the supervisor's approval, with the understanding that any confidential data saved to a USB storage device be encrypted. The IT department can assist with the use of USB devices. The Workforce is responsible for identifying if the data is confidential and therefore needs to be encrypted (see definition below).
6. Full disk encryption software should be installed on all laptop computers especially those with confidential information. The IT department will work with supervisors to identify the need to install encryption software on their staffs' laptops. IT will install the encryption software and train the staff on its use.

III. SCOPE: This policy applies to those individuals of the HHSC employees, medical staff, contractors, vendors and other agents who access HHSC's network.

IV. RESPONSIBILITIES:

- A.** Department managers or their designee will be responsible for determining workstation access for each of their staff in addition to the responsibilities listed

below for HHSC Workstation Users.

- B. The TSD shall be responsible for setting workstation configuration standards. TSD staff shall be responsible for maintaining workstations in the Corporate offices.
- C. REST staff shall be responsible for maintaining the workstations in regional facilities.
- D. HHSC Workforce responsibilities are to comply with all the provisions of this policy under Workstation Administration and Use, raise any questions relating to this policy to their supervisor or REST Director and report any non-compliance of this policy to their supervisor, REST Director or Regional Compliance and Privacy Officer.

V. DEFINITIONS

- A. Workforce - employees, volunteers, trainees, and other persons whose conduct, in the performance of work for HHSC, is under the direct control of HHSC, whether or not they are paid by HHSC.
- B. Workstation – Desktop Computer, laptop, or similar device connected to the HHSC Network
- C. Confidential – Private; requiring protection from unauthorized use or disclosure in compliance with applicable HHSC policies and federal or state laws. For example, Protected Health Information (PHI) requires protection under HIPAA and Personally Identifiable Information (PII) requires protection under Hawaii law.
- D. Protected Health Information (PHI)--PHI is any information about health status, provision of health care, or payment for health care that can be linked to an individual
- E. Personally Identifiable Information (PII)--PII is defined as the first name or initial and last name of an individual, with one or more of the following: 1) Social Security Number, 2) driver's license number, Hawaii ID number, 3) credit card or debit card number, or a financial account number with information such as PINs, passwords, or authorization codes that could gain access to the account, or other information that could cause harm to an individual or HHSC if disclosed.

VI. REFERENCES/RELATED POLICIES

- ITD 0002 - Security Configuration Management
- ITD 0017 – Electronic Mail
- ITD 0018 – Internet Use