
TITLE: **WORKSTATION USE AND SECURITY**

POLICY:

Workforce members use workstations in an appropriate and authorized manner. The authorized purpose of each workstation is to support the clinical, research, education, administrative and other legitimate business functions of the Hospital.

PURPOSE:

Define acceptable functions performed at workstations, the manner in which these are performed, and the physical surroundings of workstations that can access electronic information systems.

APPLICABILITY:

Hospital staff, employees, affiliates, owners, custodians, and users of information systems

PROCEDURE:

1. The following activities are considered examples of unauthorized uses of workstations:

    A. Violating any of institutional policies and procedures.
    B. Violating the privacy of patients and/or workforce members.
    C. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations. (e.g., installation or distribution of 'pirated' or other inappropriately licensed software).
    D. Unauthorized copying, distribution and transmission of copyrighted material (e.g., digitization and distribution of photographs from magazines, books, music, video, movies or other copyrighted sources).
    E. Intentional introduction of malicious software onto a workstation or network.
    F. Transmitting material that is in violation of institutional sexual harassment or hostile workplace policies.
    G. Making offers of products, items or services that are fraudulent and/or not related to the organizational business.

H. Intentionally causing a security incident (e.g., accessing electronic data that the workforce member is not authorized to access, logging into an account that the workforce member is not authorized to access, denying the ability of legitimate work to continue on the information systems).
I. Performing monitoring (network, computer, device, or any other) that will intercept data not intended for the workforce member unless specifically permitted by the Information Security Office.
J. Attempting to avoid the user authentication or security of workstations or accounts.
K. Allowing patients to use institutional computers for personal use unless clearly designated for such use.
L. Any unlawful activities.

This list is not intended to be an all-inclusive list. Additional criteria for acceptable use appear in ***Acceptable Use of Electronic Devices and Information policy*** (# HR-107).

2. Workforce members are responsible for reporting suspected unauthorized access/use of a workstation to the Information Technology (IT) department's Service Desk or their manager. See ***Information Security Incident Procedures policy*** (# I255).

3. Access to workstations is controlled by requiring authentication using a User Id and a password or an access device (e.g., token), unless specifically exempted based on an institutional purpose. The User Ids used are the institutional Center-wide Identifier (see *Center-wide Identifier Creation Procedure*), which enable users to be uniquely identified and their use of the systems tracked.

4. Removal of workstation access privileges for workforce members when employment or contracted services have ended are done in accordance with ***Workforce Security Clearance,* Termination and Authorization policy** (# I235).

5. Workforce members shall follow the authentication and password management requirements. See ***General Information Security policy*** (# I220).

6. Workforce members, if they used their individual User ID to sign on, should sign off when they leave their workstation. Alternately, they are instructed to activate their workstation locking when they leave their workstations temporarily. (On a Windows workstation, it is locked by pressing the *Ctrl+Alt+Delete* keys together and then select 'Lock Workstation' or equivalent button.) In general, the workstation must sign off the user after detecting 30 minutes (maximum) of inactivity, unless there are mitigating factors such as physically locked rooms and offices. Generic Ids on workstations are permitted

only if access to subsequent applications and systems require additional user-based authentication, or in special care related situations with medical devices.

7. Workstations are configured with processes defined in *Corporate Workstation Procedure*, *Corporate Mobile Devices Procedure*, and *Corporate Tablets and Smartphones Procedure*.

8. Important precautions are implemented for workstations and storage devices (e.g., laptops, USB storage devices, smart phones, tablets, portable medical equipment that store sensitive data). See ***Device and Media Controls policy*** (# I240) to follow the procedures to secure all devices and media (including personal devices) specifically to make sure that all devices and media are encrypted and password protected.

9. Every department that accesses electronic information on its workstations is responsible for periodically checking the physical protection of the workstations that is commensurate with threats and risks to the workstations at that location. Also see ***Information Security: Facility Access Control & Security policy*** (# I245). Such measures include:

   A. Locating workstations and peripheral devices in secured areas not accessible by unauthorized workforce members or other unauthorized personnel or other individuals.
   B. Positioning or shielding workstations so that data shown on the screen is not visible by unauthorized persons.
   C. Implementing additional measures including screen savers, inactivity timeout or requiring workforce members not to leave workstations unsupervised.

10. Workforce members are required to report the loss or theft of any device as specified in ***Information Security Incident Procedure policy*** (# I255)***.***

RESPONSIBILITY:

Information Security Office

REFERENCES:

All information security policies
Corporate Workstation Procedure (IT-DS-002)
Corporate Mobile Devices Procedure (IT-DS-003)
Corporate Tablets and Smartphones Procedure (IT-DS-004)
Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.310(b), 164.310(c)

REVIEW/REVISION DATE:

March 2005
June 2009
June 2011
Revised: June 2013; May 2014; **March 2015**