UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

Standard

Number: PS0004.04	Category: Physical Security	Version Date: 02/22/2010
Title: **Physical Security and Usage of End-User Computing Devices and Related Facilities**		Effective Date: 07/20/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 12/04/2009
Reviewer: HSC Chief, Information Security		Next Review: 12/04/2012

Purpose:

To establish the minimum physical security requirements to be addressed by all HSC users of information for Health Science Center End-User Computing Devices, Related Facilities and Usage in order to restrict access to authorized users and prevent tampering and theft of Information Assets.

Reference:

1. Policy PS 0004: Physical Security and Usage of End-User Computing Devices

Standard:

1. The Unit ISA and ISM may determine additional minimum device usage requirements involving physical security of HSC End-User Computing Devices that access or store only Unrestricted Information.
2. The following device usage requirements apply to End-User Computing Devices that create, access, and/or store Restricted, Sensitive, or Operational information.

	Restricted/Sensitive	Operational
Access	• All End-user Computing Devices shall have a documented system owner/user who is held accountable for the secure usage of that device. The user of each device shall be identified before the device is operated and shall be documented by the Unit ISM. (See Record Keeping below) • Personnel shall secure their work area whenever they are not available to actively monitor the area and prevent access by unauthorized individuals. • Temporary employees and	• All End-user Computing Devices shall have a documented system owner/user who is held accountable for the secure usage of that device. The user of each device shall be identified before the device is operated and shall be documented by the Unit ISM. (See Record Keeping below) • Personnel shall secure their work area whenever they are not available to actively monitor the area and prevent access by unauthorized individuals. • Temporary employees and

	contractors shall be required to follow the same access procedures for secured areas as HSC users. Unit ISA or designee shall be responsible for setting time limits on access to their work areas by these personnel and ensuring a mechanism is in place to terminate access after temporary employees and contractors cease functioning within the work area.	contractors shall be required to follow the same validation and issue procedures for secured areas as HSC users. Unit ISA or designee shall be responsible for setting time limits on access to their work areas by these personnel and ensuring a mechanism is in place to terminate access after temporary employees and contractors cease functioning within the work area.
Usage	• Personnel shall maintain knowledge of normal operations, authorized personnel and their functions, and physical security procedures for their work areas.	• Personnel shall maintain knowledge of normal operations, authorized personnel and their functions, and physical security procedures for their work areas.
Physical Safeguards	• End-user Computing Devices shall be placed outside the view or access of unauthorized users. If usage of the device does not allow this type of placement, then the device shall be set up in a manner that allows for easy monitoring by authorized users. • Work areas shall include physical barrier to access of the area such as a lock, biometric access or posted guard to prevent entry of unauthorized individuals. • Work areas shall be locked when unattended by authorized personnel. • The Unit ISA shall validate that the appropriate personnel for the area have the correct access device for work areas secured by locking mechanisms only. • Users must lock or logoff the End user Computing Device when leaving it unattended. •	• Work areas shall be locked when unattended by authorized personnel. • The Unit ISA shall validate that the appropriate personnel for the area have the correct access device for work areas secured by locking mechanisms only. • All End-user Computing Devices assigned to a single user shall save and close all files/documents and lock (where technically feasible) or logoff their workstation when unattended. All End-user Computing Devices assigned to multiple users or public access shall be logged off when unattended.

Record Keeping	• The Unit ISA shall maintain records regarding distribution of keys or access control data to personnel within their Unit.	• The Unit ISA shall maintain records regarding distribution of keys or access control data to personnel within their Unit.
Contingency	• In cases of emergency as declared by the Unit ISA or ISM, a detailed list of non-authorized personnel or organizations who access the work area shall be maintained, with the exception of situations involving possible loss of life or limb. • Within reason, users are responsible for maintaining security of information in emergency by actively monitoring non-authorized individuals coming into their work areas.	