UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

POLICY

Policy: PS0003	Category: Physical Security	Version Date: 02/22/2010
Title: **Device and Media Controls**		Effective Date: 04/01/2008
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 policy and responsibility for the receipt, removal, re-use, and disposal of any Information Asset containing Restricted or Sensitive information or the Restricted or Sensitive information itself into or out of the UF HSC or throughout the UF HSC.

Scope:

The policy applies to all Information Assets (Workstations, Laptops, PDAs, Phones, Facsimile Machines and other similar devices) that store Restricted and/or Sensitive information. Includes local, fixed and removable storage systems and media including, but not limited to, magnetic and optical, drives, removable disks, floppy disks, PCMCIA devices, USB devices, memory cards and sticks, CD-ROMs, DVDs, EPROM, magnetic tape, paper, photographs, slides, negatives, microfiche and other forms of media or storage devices both currently used and those that become available in the future.

References:

1. PS0002: Physical Security of Information Assets and Related Facilities Policy
2. PS0002.02: Physical Security of Server Rooms Standard
3. PS0003.02: Device and Media Destruction Standard
4. UF Records Management: http://www.aa.ufl.edu/aa/records/
5. Medical Records Management: http://privacy.health.ufl.edu/policies/hipaamanual/opguide/PP-OG-05-retention.pdf

Policy:

1. When Restricted and/or Sensitive information is received on media, as defined in the above scope, the information shall be either:
    a. Stored in a secure storage facility,
    b. Copied to a secured server that stores Restricted and/or Sensitive information per Standard PS0002.02,
    c. Or destroyed per Standard PS0003.02.
2. The custodian of the Information Asset is responsible for the removal and/or destruction of any Restricted and/or Sensitive information in collaboration with the owner's designee or delegate.

3. All media containing Restricted and/or Sensitive information shall be sanitized according to Standard PS0003.02 Device and Media Destruction Standard before transferring custody of the media outside of the Unit for re-use or disposal.
4. University, State of Florida and Federal records retention requirements must be met prior to destruction of information or transfer of custody of media for purposes of disposal:
    a. Owners of original copies of records must ensure the information has met the records retention requirements before requesting or authorizing the destruction of media containing original information. See UF Records Management and Medical Records Management under references above.
    b. Owners of duplicative copies of records may destroy the records when they no longer have value for the Unit without UF Records Management oversight provided the owner of the copy makes certain an original exists.
5. The custodian of the Information Asset is responsible for ensuring a retrievable copy is made of any Restricted and/or Sensitive information when required or needed and in collaboration with the owner's designee or delegate.
6. The Unit Information Security Manager (ISM) shall develop a procedure for his/her Unit to track and maintain a record of all receipt, removal, re-use, and disposal of workstations, servers and other non-portable devices covered by this policy.
7. Users are responsible for physically securing personally owned or institutionally provided portable computing devices and media. Users are also responsible for turning in these devices to their Unit ISM for proper Restricted or Sensitive information disposal per Standard PS 0003.02.
8. The Unit ISM is responsible for maintaining records of the disposal of these portable devices and media.