Policy: PS0002	Category: Physical Security	Version Date: 02/22/2010
Title: **Physical Security of Information Assets and Related Facilities**		Effective Date: 03/31/2005
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 responsibility for the physical security of HSC Information Assets and related facilities.

Scope:

This policy applies to UF HSC Units that manage any Information Assets.

References:

1. Standard PS0002.02: Physical Security of Server Rooms
2. Standard PS0002.04: Physical Security of Communications Closets
3. Standard PS0003.02: Device and Media Controls
4. Standard PS0004.02: Physical Security of End-User Computing Devices
5. Standard PS0004.04: Physical Security of End-User Computing Devices and Related Facilities.
6. Policy PS0005 – Off Site Storage Policy
7. UF Privacy Manual:
    a. Health Information and Record Management Policy
    b. Retention, Archiving, & Disposal of Patient Information

   http://privacy.health.ufl.edu/policies/hipaamanual/operational.shtml
8. UF Policies and Procedure: Finance and Accounting: Asset Management Services
   http://fa.ufl.edu/am/
9. UF Physical Plant Division Key and Lock Policy
   http://www.ppd.ufl.edu/pdf/Key_Lock_Policy.pdf

Policy:

1. It is the responsibility of the Unit Information Security Administrator (ISA), with the support of the Information Security Manager (ISM), to ensure the physical security of Unit owned and managed electronic and non-electronic Information Assets (e.g., paper, photographs, slides, negatives, microfiche, servers, workstations, printers, facsimile machines, portable devices, *etc.*) and related facilities according to the referenced Standards and in collaboration with the owners' designees or delegates.

The Unit ISA is also responsible for all record keeping and documentation relating to the referenced policies and standards.

2. The Network Service Provider is responsible for managing and physically securing communications closets and their contents according to Standard PS0003: Physical Security of Communications Closets. The Network Service Provider is also responsible for all record keeping and documentation relating to the referenced policies and standards.
3. It is the responsibility of the UF Privacy Office, through the roles of the Institutional Privacy Officer and HSC Medical Records Coordinator, to establish protections through policy and guidelines to managers for the physical safeguards of non-electronic Restricted information and to undertake related compliance evaluation.