Policy: GP0003	Category: General Provisions	Version Date: 09/02/2009
Title: **Information Security General Provisions**		Effective Date: 03/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 07/17/2009
Reviewer: HSC Chief, Information Security		Next Review: 07/17/2012

Purpose:

To delineate the general provisions of information security.

Scope:

This policy applies to all individuals and UF HSC Units, including, but not limited to UF HSC faculty and staff, volunteers, students, and third parties, who have been granted access to any UF HSC Information Asset.

Reference:

1. Standard GP0003.02: Information Classification
2. Standard GP0003.04: Information Security Program Definitions
3. Standard GP0003.06: Information Security Violation Levels
4. Standard GP0003.08: Report Distribution and Submission Deadlines

Policy:

1. Overall responsibility for determining the security classification of information rests with the owner's designee or delegate responsible for that information. The implementation of security measures may be delegated as appropriate, but such delegation does not result in relinquishing responsibility.
2. The information owner's designee or delegate should refer to Standard GP0003.02: Information Classification, for guidance in establishing security requirements. Protected Health Information (PHI) and Personally Identifiable Information (PII) and Private Education Records (PER) are classified as Restricted.
3. All personnel given access to information assets share responsibility for ensuring the appropriate security of information and addressing security lapses or breaches. Any observed violation of the Information Security Program must be reported to the Unit Information Security Administrator or the Unit Information Security Manager.
4. The custodian must provide appropriate safeguards and system monitoring as defined by the HSC Information Security Policies and Standards, to protect Information Assets from misuse in accordance with the needs defined by the owner's designee or delegate (see Standard GP0003.02, Information Classification).
5. Access to Restricted Information Assets shall be authorized based on the individual's role and responsibilities and the classification of the Information Asset. Access must

be properly documented, authorized and controlled.

6. Users are responsible and individually liable for:
    a. Managing their use of UF HSC Information Assets and are accountable for their actions relating to security.
    b. Protecting passwords, Personal Identification Numbers (PIN), Security Tokens, and other Information Asset security procedures and devices from use by, or disclosure to, any other individual or organization.
    c. Not bypassing or disabling security controls.
    d. Surrendering all property and components of UF HSC Information Assets which are in their possession upon termination of their relationship with UF HSC, or change in assignment or duties resulting in access being unnecessary or inappropriate. All pertinent security policies apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated or altered relationship.