Policy: CP0001	Category: Contingency Planning	Version Date: 02/22/2010
Title: **Maintaining Information Security During a Disaster**		Effective Date: 03/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 06/30/2009
Reviewer: HSC Chief, Information Security		Next Review: 06/30/2012

Purpose:

To specify required treatment of information assets and systems in the case of an emergency or other event resulting in the loss, destruction, theft or corruption of information assets, an inability to access information that cannot be resolved in a reasonable time period, or damages to systems which are necessary for the maintenance of confidentiality, integrity and availability of information. These events shall be referred to collectively and individually as "disaster."

Scope:

All UF Health Science Center (HSC) information assets and systems. References to contingency planning and disaster planning are limited to plans regarding the treatment of information assets per the above purpose. Business resumption in this context is limited to, and refers specifically to, the establishment and implementation of procedures to enable continuation of critical business processes for protection of the security of information assets while operating in an emergency mode as dictated by the above circumstances. Note that "critical business processes" relate to the protection and security of information assets, and are not the same thing as "crucial" assets as defined in Policy CP0002.02.

Reference(s):

1. Policy CP0002.02: Risk Assessment – Mission Crucial System.
2. Policy GP0001: Applicable Information Security Regulations/Laws/Policies.
3. Policy GP0002: Information Security Program Compliance.
4. Standard CP0002.04: Contingency Planning Template.
5. Standard GP0003.02: Information Classification.
6. Standard GP0003.06: Information Security Violation Levels.

Policy:

1. In the case of disaster:
    a. During all phases of an anticipated and / or unanticipated disaster (including, but not limited to, preparation for an impending event, the immediate aftermath of the event, implementation of contingency plans, subsequent

recovery and return to normal operation) all policies, laws and regulations required to be followed by Policy GP0001 shall remain in effect.

b. Written procedures to enable continuation of critical business processes for the protection of the security of all information classified as Restricted shall be maintained. In support of this requirement:
    i. Copies of these written procedures shall be retained offsite.
    ii. Software and systems that are necessary for continuation of these business processes shall be documented as a part of these procedures. The procedures shall specify how, and in what time frame after their loss or compromise the functionality of these processes shall be restored. Documentation shall include a mapping of all applications and systems to the Restricted data affected. As an alternative to determining which software, systems and data are crucial or which contain Restricted data, all systems may be treated as if they are crucial and contain Restricted data.

2. Theft of data shall be treated as a security incident per Policy GP0002: Information Security Program Compliance. If data have been stolen, there has been unauthorized access to, or use of, the data. Its integrity and validity shall be verified prior to further use.