UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

POLICY

Policy: CP0002	Category: Contingency Planning	Version Date: 02/22/2010
Title: **Contingency Plan**		Effective Date: 03/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 07/08/2009
Reviewer: HSC Chief, Information Security		Next Review: 07/08/2012

Purpose:

To put in place a contingency plan to be exercised in the event of a disaster as defined in Policy CP0001.

Scope:

The scope of this contingency plan is limited to the information assets of the Unit. Its primary concern is maintaining the confidentiality, integrity, availability, and reliability of information assets in the event of disaster.

Reference(s):

1. Policy CP0001: Maintaining Information Security During a Disaster.
2. Policy CP0002.02: Risk Assessment - Mission Crucial Systems.
3. Policy GP0002: Information Security Program Compliance.
4. Standard CP0002.04: Contingency Planning Template.
5. Standard GP0003.08: Report Distribution and Submission Deadlines

Policy:

1. General:
    a. Each Unit shall maintain a written contingency plan. The format of standard CP0002.04 may be used. It is the intent that Standard CP0002.04 provides a format that facilitates meeting all requirements of contingency planning policy. It is the responsibility of the Unit Information Security Administrator (ISA) to ensure that all requirements of the contingency planning policies are satisfied.
    b. Should an alternative to the format of Standard CP0002.04 be used, all of the same information must be included in the plan.
    c. The contingency plan shall specifically address:
        i. Restoration of critical business processes per Policy CP0001.
        ii. Recovery of assets classified as crucial per Policy CP0002.02.
        iii. Preparation for a possible impending disaster, such as an approaching hurricane.

2. Responsibility:
    a. The Unit ISA shall be responsible for:
        i. Ensuring that the contingency plan contains all required elements.
        ii. Complying with all contingency planning policies.
    b. The Unit Information Security Manager (ISM) is responsible for advising the Unit ISA with regard to the technical aspects of these duties. If, in the opinion of the ISM, sufficient action is not being taken with respect to these recommendations, it is the Unit ISM's responsibility to inform the Dean, Director or Department Chair in writing.
    c. The contingency plan shall designate who in the Unit is authorized to put the contingency plan into operation. This person will be designated as the Unit's Contingency Plan Coordinator.
3. Plan review:
    a. This plan shall be reviewed and updated, at a minimum:
        i. Annually
        ii. In response to environmental or operational changes which affect any part of the plan.
        iii. Following exercise of any portion of the plan which reveals deficiencies.
4. Documentation:
    a. Offsite copies of the latest revision of this plan shall be maintained by:
        i. The Unit Information Security Administrator.
        ii. Information Security Manager.
        iii. The senior person in the Unit, for example, the Dean, Director or Department Chair.
        iv. The Health Science Center HSC Chief, Information Security.
        v. Other key personnel responsible for execution of the plan, such as the Contingency Plan Coordinator and their backups.
    b. Reviews per section 3 of this policy shall be accomplished by the Unit ISA, who shall sign and date the plan signifying such review.
    c. The plan shall be approved annually, subsequent to review by the Unit ISA, by the senior person in the Unit, who shall sign and date the plan signifying such approval.
    d. A copy of the most recent version of the plan, as approved per section 4.c. of this policy, shall be forwarded to the HSC Chief, Information Security by the Unit ISA annually per the schedule of Standard GP0003.08. Copies of plan updates made between formal reviews shall also be forwarded to the HSC Chief, Information Security. The HSC Chief, Information Security shall maintain a file of the most current version of the contingency plans for all Units both onsite and offsite.
    e. Reviews and changes to the plan made between annual reviews shall be approved by the Unit ISA. A time-date stamped record of changes and

reviews shall be maintained at the front of the document immediately behind the cover page.

5. Training
    a. The Unit ISA is responsible for conducting training annually and at each change in the plan for those who have responsibilities under the plan. Training on changes need only be provided to personnel directly affected.
    b. Recovery teams and users shall be trained to understand and know their role in the business recovery process.
6. A record of training and who attended, and a summary of the content of the training shall be maintained by the Contingency Plan Coordinator.
7. Testing
    a. The plan shall be exercised on an annual basis. A written determination shall be made by the Contingency Plan Coordinator and approved by the senior person in the Unit documenting per standard CP0002.04 what portions of the contingency plan, if any, are to be exempted from this requirement.
    b. It is permissible to exercise various elements of the plan in phases, or at different times during the year. This is not an exception to the requirement to exercise the plan.
8. Reporting
    a. Completion of annual training and exercise of the plan, and documentation of any exceptions, shall be forwarded to the HSC Chief, Information Security annually, per the schedule of Standard GP0003.08.
    b. Report of annual completion of contingency plan review shall be forwarded to the HSC Chief, Information Security per the schedule of Standard GP0003.08.
    c. The HSC Chief, Information Security shall provide within 30 days of the above reporting deadline, to Distribution 4 of Standard GP0003.08, a summary report of:
        i. Those Units that have not completed annual training, or have failed to report its completion per section 7.a. of this policy.
        ii. All approved exceptions to exercise of contingency plans per section 7.a. of this policy.
        iii. All Units reporting that the contingency plan has not been exercised, or failing to report on exercise of the contingency plan per section 7.a. of this policy.
        iv. Status of Unit review and update of contingency plans per section 7.b. of this policy.
    d. The Senior Vice President of Health Affairs shall initial the summary report and return it to the HSC Chief, Information Security for retention. The responsible person in Units out of compliance with review requirements shall be subject to the sanctions policy, Policy GP0002.