Purpose:

The purpose of this policy is to protect the ability of the university to continue to operate when Information Systems suffer disruptions or damage. Contingencies could include natural disasters, malicious activity and human error.

Scope:

This policy applies to all University of Florida units.

Policy:

1. Units will maintain a written contingency plan covering business critical information systems, components and processes. The plan includes:
   a. A description of essential business functions, and the systems, components and processes supporting them.
   b. Recovery Point Objectives and Recovery Time Objectives for each function.
   c. Identification of assigned individuals and their roles and responsibilities.
   d. Methods for appropriate maintenance of information security.
   e. Procedures for interim recovery and final restoration of essential business functions.

2. Unit personnel will be trained to fulfill their roles in the contingency plan.

3. Units will conduct exercises of contingency plans.

4. Plans are reviewed and updated periodically, to reflect changes in personnel, business functions or information systems, or results of exercises.
Policy: Contingency Plans

Responsibilities:

1. Information Security Administrators (ISAs) are responsible for developing, exercising and maintaining unit contingency plans.

2. Information Security Managers (ISMs) are responsible for providing support to their ISA in development of Contingency Plans.

3. The Vice President and CIO is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

Authority:

UF-1.0102: Policies on Information Technology and Security

References:

NIST 800-53 revision 3: CP-2, CP-3, CP-4, CP-7, CP-8