UF UNIVERSITY of FLORIDA
Information Technology

# *Policy:* Backup and Recovery

## Purpose:

The purpose of this policy is to protect University Data from loss or destruction by specifying reliable backups that are based upon the availability needs of each unit and its data.

## Scope:

This policy applies to all University of Florida Data and the Information Systems used with it.

## Policy:

1. University Data is backed up in a manner sufficient to restore any or all of an Information System in the event of a data loss, according to Recovery Time Objectives and Recovery Point Objectives.

2. Backups are periodically tested to ensure that backups are sufficient and reliable.

3. Backup systems and media protect the confidentiality, integrity and availability of stored data.

4. Written procedures are maintained to allow unit personnel to recover data in the event of an emergency.

## Responsibilities:

1. Information Security Administrators (ISAs) are responsible for establishing Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), in conjunction with data users and owners, for all University Data collected, stored or maintained by the unit. ISAs should verify that Data used by the unit, but collected, stored or maintained by others, have appropriate backup plans.
2. Information Security Managers (ISMs) are responsible for implementing backup systems and processes to ensure that RTO and RPO can be met for all data collected, stored or maintained on unit Information Systems. ISMs document backup system operation and test recovery capability.

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-9, CP-10, CP-6