# INFORMATION TECHNOLOGY DISASTER RECOVERY AND DATA BACKUP POLICY

## SPECIFIC AUTHORITY

Florida Statutes, Chapter 252, Emergency Management
Leon County Comprehensive Emergency Management Plan
Florida State University Master Plan
Florida State University Emergency Management Plan (OP-G-4)
Florida State University Continuation of Operations Plan (COOP) (OP-G-4.1)

## OBJECTIVE

The purpose of the Information Technology Disaster Recovery and Data Backup Policy is to provide for the continuity, restoration and recovery of critical data and systems. Campus Units need to ensure critical data is backed up periodically and copies maintained at an off site location. Campus units must develop and maintain a written business continuity plan for critical assets that provides information on recurring backup procedures, and also recovery procedures from both natural and man made disasters.

## A. SCOPE

The data backup section of this policy applies to all campus entities and third parties who use computing devices connected to the university network or who process or store critical data owned by the Florida State University. Campus users are responsible for arranging adequate data backup procedures for the data held on IT systems assigned to them.

The disaster recovery section of this policy apply to all Network Managers, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

The Office of Technology Integration (OTI) is responsible for the backup of data held in central systems and related databases. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the university falls entirely to the user. Campus users should consult their departmental IT lead or system administrator about local back-up procedures.

## B. DATA BACKUP

All backups must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up. (Ensure this includes all patches, fixes and updates).
- Records of what is backed up and to where must be maintained.
- Records of software licensing should be backed up.
- The backup media must be precisely labeled and accurate records must be maintained of back-ups done and to which back-up set they belong.
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency.

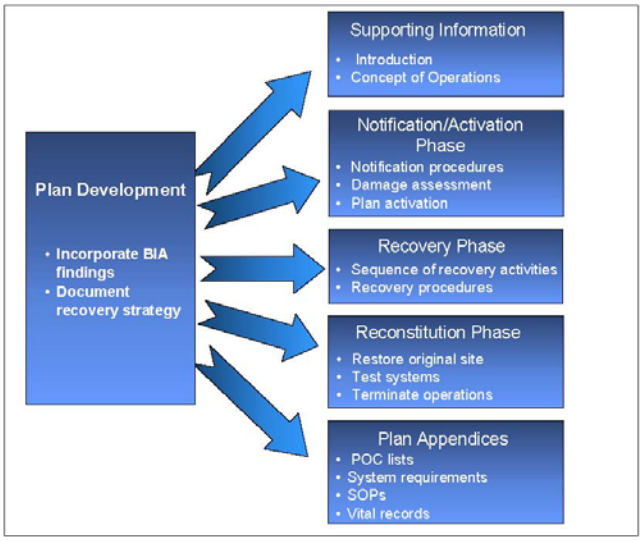
Note: For most important and time critical data, a mirror system, or at least a mirror disk may needed for a quick recovering.

## C. DISASTER RECOVERY

Best Practice Disaster Recovery Procedures. A disaster recovery plan can be defined as the on-going process of planning developing and Implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

Campus Unit should develop IT contingency plans as a critical step in the process of implementing a comprehensive contingency planning program. The plan should contain detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually the more detailed the plan is, the less scalable and versatile the approach. The information presented here is meant to be a guide; however, the plan format in this document may be modified as needed to better meet the user's specific system, operational, and organization requirements.

There are five main components of the IT contingency plan. The Supporting Information and Plan Appendices provide essential information to ensure a comprehensive plan. The Notification/Activation, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency. IT contingency plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used.




IT Contingency Plan Components

*Source NIST Sp 800-34*

**D. IMPLEMENTATION**
Effective Date: July 1, 2006

**E. REVIEW AND UPDATE**
This policy shall be reviewed and updated on an annual basis, or as special events or circumstances dictate.

**F. RELATED STATE, LOCAL AND UNIVERSITY REFERENCES.**
University faculty, staff, students, and employees are bound by all applicable laws, rule, policies, and procedures. This policy is not intended to limit the applicability of any law or policy and does not preclude University units and related affiliate organizations from implementing additional supplemental, or more stringent safeguards.

State and Local Government references:
Florida Statutes, Chapter 252, Emergency Management
Leon County Comprehensive Emergency Management Plan

University Policy references:
OP-F-6 Destruction/Shredding of Confidential Documents and Records
OP-F-7 Policy on Safeguarding of Confidential Financial and Personal Information