Southern University Law Center
Policy #IT0003

Title: Disaster Recovery & Backup Policy

Authority: Department
Original Adoption: 5/29/2007
Effective Date: 5/29/2007
Last Revision: 9/17/2012

1.0 Purpose:

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. Information Technology Support Services need to ensure critical data are backed up periodically and copies maintained at an off-site location. ITSS 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.

2.0 Scope:

The data backup section of this policy applies to all campus entities and third parties who use computing devices connected to the Southern University Law Center (SULC) network or who process or store critical data owned by the Law Center. SULC users are responsible for arranging sufficient data backup procedures for the data held on IT systems assigned to them.

The disaster recovery section of this policy applies to the Law Center IT department responsible for Law Center IT controlled critical systems, communications infrastructure, and data processed, stored, and managed either onsite or remotely. Note: critical is defined as those systems, data, or information that enables continuity or resumption of critical business processes in the event of a disaster.

ITSS 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. SULC users should consult the ITSS Department about local back-up procedures.

3.0 Definitions:

4.0 Policy:

CRITICAL 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.

DISASTER RECOVERY

Best Practice Disaster Recovery Procedures. A disaster recovery plan can be defined as the ongoing 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.

SULC 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.