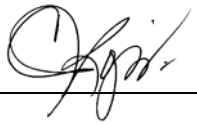
"Linking Citizens of Louisiana with Opportunities for Success"

Southern University and A & M College System
AGRICULTURAL RESEARCH AND EXTENSION CENTER
Ashford O. Williams Hall
P. O. Box 10010
Baton Rouge, LA 70813
(225) 771-2242
(225) 771-2861 Fax
www.suagcenter.com

DATE: **September 9, 2011**
SUBJECT: **IT Disaster Recovery, DATA Storage and Backup Policy**
AUTHORIZATION: **Christopher J. Rogers, Director of Technology Services**



Below are statements of policy regarding user data storage and backups. In general, Information Technology (IT) strongly recommends storing user-created data on IT-administered file servers and to create additional backup copies of the critical data he or she creates, maintains, or modifies. Disaster Recovery applies to all Network Administrators, and support staff who are responsible for critical systems or for a collection of critical data held either remotely on a server. *(Note: Critical is defined as those mission critical systems, data or information that enables continuity or resumption of business processes in the event of a disaster).* The procedures used by individuals for creating these additional backup copies may differ based on the value of the data as assigned by the user, how frequently the data is modified, and other factors. Accidents, computer equipment malfunction or failure, and human error are the most common causes of data loss. In most cases, damaged or lost data cannot be restored at any cost. In any case, don't rely solely on a single copy of data stored on your PC, a file server, or any other media, if losing that data would cause you distress.

A number of alternatives for storing backup copies of user data are available. For individual, small sized files, Jump Drives (USB Drives – 4GB or Higher) are reasonable. For moderate numbers or very large amounts of data, External hard drives (160GB or Higher) and/or Virtual Storage, i.e. Drop Box) are quite adequate. In many cases, a combination of IT-supported file server storage, the local desktop hard drive, and portable media can be used to provide adequate backup of critical data files.

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.

The Southern University AgCenter has developed IT contingency plans as a part of the campus Emergency Preparedness Plan. This is 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.

Data Storage

- IT's standard configuration of desktop computer operating systems and application software stores user data in a single directory tree.
- User data should be stored on an IT-administered file server in order to receive minimal, regular backups of data. Although users should not rely solely on file server backups, neither should they rely solely on desktop system hardware or the backup copies they store.

Backup Data

- Backups of file servers, taken by IT, are not intended for restoring individual users' data files, but rather for recovering from file system damage caused by equipment and/or software failure, system upgrade error, and minor disasters such as power failures.
- Copies of the back-up media, together with the back-up record, are 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 be needed for a quick recovery*
- In some cases, for some users, the IT backup procedures are adequate insurance for data. In other instances, these procedures are not adequate. It is the user's responsibility to determine what constitutes adequate backup coverage for his or her data.
- *Every computer user is responsible for determining and maintaining adequate backup copies of critical, important, irreplaceable data files.* For extremely valuable data, multiple copies stored in multiple locations is strongly recommended. Data stored on typical media such as removable hard drives, jump drives, optical disk (CD-ROM/DVD), can be damaged by heat, magnetic fields, oxidation, and in general, the aging process, so copies cannot be relied upon indefinitely.

If you have specific questions or need assistance, please call the Office of Technology Services at (225) 771- 5996.