

## Back Up Addendum

<b>Doc. Version:</b>	1.0.0	Page 1 of 2	
<b>Revised by:</b>	John Baxter	<b>Date:</b>	8/29/04
<b>Effective Date:</b>	10/12/2004		
<b>Approval:</b>	W. R. Rice, Chancellor & C. Fitch, CIO		

### Overview

This Addendum addresses the need to protect and safeguard UTHSC data by assuring completed and properly stored back ups of critical data.

### Purpose

The purpose of this Addendum is to ensure the availability, reliability and integrity of university information resources by establishing requirements for computers containing information relevant to university business, projects and programs, and/or intellectual property.

### Scope

This Addendum refers to units, students, employees, contractors and other users of university computer systems including file servers, workstations and/or networks.

### Definitions

- Unit:** A general term to refer to an organizational group of faculty, staff, students, contractors, etc. (e.g. department, division, section, office, college, etc.)
- Off-site:** An area sufficiently convenient to, but remote from the computing device(s), to assure that, in the event of a disaster or of damage to the computing device or to the primary site, important support items if properly stored can be secured in protected storage to prevent physical and electronic loss or damage to the stored items (e.g., backups, archives, other media, documentation, spares, important disposables, etc.).
- Backup:** The process of duplicating important data on removable media for the purpose of safety of the data. Should the original information (on the computing device) become corrupted or lost, the information can be retrieved from the backup media.
- Archive:** The process of storing files and/or records (usually on removable media) that have been determined to have sufficient historical or other value to warrant their long term or permanent preservation.

### Policy

1. It is the responsibility of server system managers and of desktop end users to backup, on a defined and regular basis, any sensitive or critical University related information and data on all computers for which they are responsible.
2. Each unit must have a written backup plan including a backup schedule, a restore plan and procedure, and a list of university sensitive and critical applications.
3. Backups should be initially and periodically tested and validated to assure that the information they contain is complete and that it can be restored.
4. Units should consider their current electronic archiving process while developing their backup plan.

## Back Up Addendum

<b>Doc. Version:</b>	1.0.0	Page 2 of 2	
<b>Revised by:</b>	John Baxter	<b>Date:</b>	8/29/04
<b>Effective Date:</b>	10/12/2004		
<b>Approval:</b>	W. R. Rice, Chancellor & C. Fitch, CIO		

5. Units cannot use the backup process as an electronic archiving method; a separate electronic archiving process and plan must be developed.
6. The backup plan must be reviewed annually and periodically tested by the unit designated system administrator.
7. Each unit must maintain a notification list of designated staff to be contacted in an emergency. A copy of this list must be kept in a secure location, such as with off-site backups, and be readily accessible in case of an emergency.
8. At a minimum, modified data must be backed up at appropriate intervals and a full system backup must be stored off-site.
9. University sensitive and critical data should be backed up and stored off-site regardless of where it resides (e.g. an off-campus location).
10. On site and off site backup copies shall be stored in a physically secure location in a manner that will prevent damage to media and to data.

### Guidelines

It is recommended units maintain a list of hardware specifications for all critical systems to insure appropriate replacement hardware can be provided in case of a disaster. System administrators (or staff designated as such) should be trained in the use of current backup hardware, software and policies. Units should insure users are trained in proper workstation backup procedures.

It is also recommended units maintain bootable media containing an emergency recovery configuration and backup software. Units should test the viability of the media to recover the system and load the backup software in order to perform a full system restore.

A consideration for a unit's electronic archiving plan is to designate certain directories or drives for electronic archiving. These directories or drives should not contain e-mail or documents considered temporary. Another consideration for a unit's electronic archiving plan is to include a migration plan for transferring data from one media to another as technology changes.

### Enforcement

Reference **Enforcement in Acceptable Use document.**

### Additional Information

Any inquiries relating to this Back Up Policy should be directed to the Security Director.