Section:	Information Security	Revised:	December 2004
Guideline:	Backup	Template Provider:	Information Security Office
Description:	***Security Guidelines: are <u>recommended</u> processes, models, or actions to assist with implementing procedures with respect to the subject.***		

BACKUP

SECURITY GUIDELINE

The pages following represent a template to be used by HSC Organizations in developing their own backup procedures. Backup procedures are required by some local, state, and federal requirements based on business risk or criticality of information. The template describes backup process considerations, solutions, and documentation needed to fulfill regulatory requirements. The pages following are designed so HSC Organizations may print/file the document, then fill in the blanks for HSC Organization specific information.

Note: Service Level Agreements with Computing Resources can also facilitate HSC Organization backup needs or assist with backup media storage.

BACKUP PROCEDURES

for the

(Fill-In-Blank) HSC Organization

Updated MONTH DD, YYYY

Maintained by:

Name:	
HSC Organization:	
Phone:	
Email:	

Table of Contents

1. Policy

It is the policy of The University of Texas Health Science Center (UTHSCSA) to protect its information and to recover from interruptions of vital University operations. The Health Science Center's (HSC) Organization _____ is taking responsibility for the development and implementation of backup procedures that are consistent with the overall policies and procedures guiding the University. Furthermore, our organization is committed to employ all appropriate backup strategies for anticipating and controlling crisis situations.

2. Purpose

Electronic backups enable the recovery of data, systems, and applications in the case of events such as natural disasters, system disk drive failures, compromises, data entry errors, or system operations errors. Backups facilitate the availability, restoration, and performance of essential functions during any emergency or situation that may disrupt normal operations. Backup considerations may include but not limited to: servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology). Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information. Information resources backup and recovery process for each system must be documented and periodically reviewed.

3. Backup Planning

The following questions should be considered when developing a backup plan:

- Where will media be stored?
- What data should be backed up?
- How frequent are backups conducted?
- How quickly are the backups to be retrieved in the event of an emergency?
- Who is authorized to retrieve the media?
- How long will it take to retrieve the media?
- Where will the media be delivered?
- Who will restore the data from the media?
- What is the media-labeling scheme?
- How long will the backup media be retained?
- When the media are stored on-site, what environmental controls are provided to preserve the media?
- What is the appropriate backup media?
- What types of media readers are used at the alternate site?
- What are the costs for varying backup solutions?

- What is the business impact for loss of data or availability?

TABLE 3.1	*HSC Organization System/Component Backups*

The _____ HSC Organization has determined based on business needs and risks to backup the following systems or components:

SYSTEM/COMPONENT

1. _____
2. _____
3. _____
4. _____
5. _____

4. Backup Media

Backups can be stored on various media such as:

- **Floppy Diskettes.** Floppy diskette drives are becoming less standard with most computers and these drives have a low storage capacity and are slow.
- **Tape Drives.** Tape drives are not common in desktop computers, but are an option for a high-capacity backup solution. Tape drives are automated and require a third-party backup application or backup capabilities in the operating system. Tape media are relatively low cost.
- **Removable Cartridges.** Removable cartridges are not common in desktop computers and are often offered as a backup solution as a portable or external device. Removable cartridges, such as Iomega Zip® and Jaz® storage drives, are more expensive than floppy diskettes and are comparable in cost to tape media depending on the media model and make. However, removable cartridges are fast, and their portability allows for flexibility. The portable devices come with special drivers and application to facilitate data backups.
- **Compact Disk.** CD, read-only memory (CD-ROM) drives come standard in most desktop computers; however, not all computers are equipped with writable CD drives. CDs are low-cost storage media and have a higher storage capacity than floppy diskettes. To read from a CD, the operating system's file manager is sufficient; however, to write to a CD, a rewritable CD (CD-RW) drive and the appropriate software is required.
- **Digital Versatile Disc.** DVD is an optical disc technology with gigabyte storage capacity and can facilitate video, audio or other information storage. This technology

has a higher capacity than CDs and is also more expensive; however, it is becoming a standard with new desktops.

- **Network Storage.** Data stored on networked PCs can be backed up to a networked disk or a networked storage device:
- **Networked disk.** A server with data storage capacity is a networked disk. The amount of data that can be backed up from a PC is limited by the network disk storage capacity or disk allocation to the particular user. However, if users are instructed to save files to a networked disk, the networked disk itself should be backed up through the network or server backup program.
- **Networked storage device.** A network backup system can be configured to back up the local drives on networked PCs. The backup can be started from either the networked backup system or the actual PC.
- **Replication or Synchronization.** Data replication or synchronization is a common backup method for portable computers. Handheld computers or laptops may be connected to a PC and replicate the desired data from the portable system to the desktop computer.

TABLE 4.1	*HSC Organization Backup Media Specification*

The _____ HSC Organization has determined the appropriate backup media as follows:

	SYSTEM/COMPONENT	**BACKUP MEDIA**
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____

5. Backup Methods

A combination of backup methodologies can be used depending on the system configuration and recovery requirements. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

System Backups

- **Full.** A full backup captures all files on the disk or within the folder selected for backup. Because all backed-up files were recorded to a single media or media set, locating a

particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.

- **Incremental.** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.
- **Differential.** A differential backup stores files that were created or modified since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup will save the file each time until the next full backup is completed. The differential backup takes less time to complete than a full backup. Restoring from a differential backup may require less media than an incremental backup because only the full backup media and the last differential media would be needed. As a disadvantage, differential backups take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.

Data Backups

- **Continuous.** Continuous data backups can be achieved by utilizing technology that writes data simultaneously to an alternate system. This method is most commonly used for data recovery. Examples include:
    - ***Disk replication*** - data is written to two different disks to ensure that two valid copies of the data are always available. The two disks are called the protected server (the main server) and the replicating server (the backup server). Disk replication can be implemented locally or between different locations. Disk replication techniques include: RAID technology, mirroring, and shadowing.
    - ***Electronic vaulting and remote journaling*** - are similar technologies that provide additional data backup capabilities, with backups made to remote tape drives over communication links. Remote journaling and electronic vaulting enable shorter recovery times and reduced data loss should the server be damaged between backups. With electronic vaulting, the system is connected to an electronic vaulting provider to allow backups to be created off-site automatically. The electronic vault could use optical disks, magnetic disks, mass storage devices, or an automated tape library as the storage devices. With this technology, data is transmitted to the electronic vault as changes occur on the servers between regular backups. These transmissions between backups are sometimes referred to as electronic journaling.

- **Scheduled.** Scheduled data backups can be achieved by utilizing scripts, backup software, or operating system tools for coping files to alternate systems. This process may be schedule or manual.

TABLE 5.1	*HSC Organization Backup Methods and Frequency*

The _____ HSC Organization has determined the appropriate backup method as follows:

	SYSTEM/COMPONENT	**BACKUP METHOD**	**FREQUENCY**
1.	_____	_____	_____
2.	_____	_____	_____
3.	_____	_____	_____
4.	_____	_____	_____
5.	_____	_____	_____

6. Backup Storage

Based on data criticality, storage of backup media may include multiple storage strategies such as both onsite and offsite. When selecting a storage facility or service, the following criteria should be considered:

- **Geographic area**—distance from the organization and the probability of the storage site being affected by the same disaster as the organization
- **Accessibility**—length of time necessary to retrieve the data from storage and the storage facility's operating hours
- **Security**—security capabilities of the storage facility and employee confidentiality, which must meet the data's sensitivity and security requirements
- **Environment**—structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls)
- **Cost**—cost of shipping, operational fees, and disaster response/recovery services.

For critical information, it is good business practice to store backed-up data offsite. **Computing Resources** services or Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. If using offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility. When the data is required for recovery or testing purposes, the organization contacts the storage facility requesting specific data to be transported to the organization or to an alternate facility. Commercial storage facilities often offer media transportation and response and recovery services.

TABLE 6.1 *HSC Organization Backup Storage Strategy*

The _____ HSC Organization has determined the appropriate backup storage strategy is:

	SYSTEM/COMPONENT	BACKUP STORAGE STRATEGY
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____

7. Backup Labels

Backup media stored should have appropriate labeling to managing tape ownership, sensitivity and rotation such as the following:

- HSC Organization Name:
- HSC Organization Location
- System or Component Name:
- Creation Date:
- Expiration Date:
- Data Classification:
- Contact Information:

8. Backup Testing

Testing is an integral part of ensuring your backups are good and available when needed. Testing should be done routinely. When testing backups, extra caution should be used not to impact your operations. When, where, and how are important decisions before attempting to validate your backups. Document for backup testing per system or component is maintained in Appendix A.

TABLE 8.1	*HSC Organization Backup Testing Strategy*

The _____ HSC Organization has determined the appropriate backup testing strategy as follows:

	SYSTEM/COMPONENT	**TEST PLAN (When, Where, How)**
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____

9. Specific Operating System References

More information is available for specific operating systems from vendor supported websites. Some of these websites contain specific recommendations, procedures, or scripts for specific operating systems. Below are the major websites for assistance:

http://www.microsoft.com/

http://www.redhat.com/

http://www.sun.com/

http://www.apple.com/

APPENDIX A - BACKUP TESTING LOG

System/Component	Test Date	Results	Facilitator

APPENDIX B - Additional Supporting Documents