BACKUP BEST PRACTICES

To protect against hardware failure, disaster, malicious tampering, or even accidental deletion, it is recommended that all TLN libraries implement a data backup and recovery plan.

Best Practices for Backing up Data

Files/Application/OS Data Only:

- In a library that utilizes servers, library staff computers should be configured to save data to a central server, allowing 1 backup to be performed on a central server (or a few servers) and not individual workstations. Important data should be backed up to an attached media drive. As part of the library's disaster recovery plan, a method of restoring the operating system and important programs needs to be addressed in the case of a hardware failure.

- In smaller libraries that do not employ servers, individual workstations will need to have their data backed up individually. A backup policy should be put in place that encourages users to back up their own data daily to a network attached storage device or removable, rewritable media. A method of restoring the operating system and important programs needs to be addressed in the case of a hardware failure.

Full System Backup - disk imaging:

- Servers: backing up the entire server by imaging the hard drive(s) will not only protect against lost/corruption of programs (and not just data), but can speed up recovery time as it combines system recovery and data recovery.

- Workstations: regular disk imaging can also be employed on workstations; however cost will be higher as software will need to be installed on every workstation. Backup media cost will also be higher.

Periodic offsite backups should be made to facilitate recovery in the event of a fire situation that destroys/damages the server and the backup media. Backup copies of all important software should also be kept offsite in case a full system recovery is necessary.

In addition to performing backups, a regular schedule should be set to test the integrity of your backups.

It is recommended that each library have a written backup and restore procedure in place as part of disaster recovery procedures.

Best practices for frequency of backups

For a library using centralized servers, some method of backup should be performed every day your library is open. You can choose to do a full backup every day or a full backup once a week followed by incremental backups the rest of the week – depending on your situation (backup software, amount of data, size of backup media, etc.)

Backups on personal/shared workstations should be performed at the end of each workday when that system is used.

Recommendation for backup devices

There are several backup media/devices available, depending on the type of backups being performed, the system being backed up, and the amount of data being backed up.

Server Backup:
Magnetic tape

External Hard drive:
External hard drives are inexpensive alternatives to magnetic tape drive systems. Hard Drives can be connected to a server's USB, firewire, or eSATA port and can be easily removed from the server area or building for security purposes.

Workstation Backup:
Network attached storage device – a networked hard drive to which multiple workstations could connect and backup their data.

If a network attached solution is not available the following removable media could be used:
Flash Drive
External Hard drive
CD-R/DVD-R
CD-RW/DVD-RW

Recommended Backup Hardware/Software

Hardware
Dell LTO external tape drive

Software
Symantec Backup-Exec, Symantec Backup-Exec System Recovery