# BACKUP POLICY

The entire user data on all systems is backed up to tape libraries, located in separate space from the server room. This provides the protection in the cases where you have deleted the file by accident or made modifications that you want to rollback or get back to certain older version of your files. Also, in the cases that there is a serious server crash or system crash, the tape backups provide data protection (e.g. a hard drive failure will not harm even the consistency of the data in the disk systems).

The backups are done daily as well as weekly basis, and their success is controlled from the reports. The tape generally allows recovery of any user file or databases to any point in time within the last year, even if the file had been deleted.

Records of what is backed up and to where must be maintained. Records of

software licensing should be backed up.

Copies of the backup media, together with the backup record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from 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.

Files on user file systems are backed up to tape mainly so they can be restored in case of a disk failure, accidental deletion, or intentional deletion by a hacker. You should not rely on the backup system to recover your files after you intentionally delete them (although in most cases the backup system should be able to recover them), rather you should put your files on your own backup tape that you keep. File systems not listed in the user file systems list are NOT backed up.

**Current Backup Procedures**

Daily Backup Procedure

- Odin Manager folder
- Odin Database

Weekly Backup Procedure

- Odin Manager
- Odin Database
- E-Hastaksar
- NSE TAP Server

- BSE IML Server
- Web Server
- Mail Servers (mail.ansplshares.com & mail.anspl.net)
- Company's User Data
- Tape storage media is removed from the machine room each morning after the backups complete and stored in a fire safe in the same building.
- Each Saturday media for the previous day's backup is removed to an offsite fire safe for longer term storage.
- A full cold backup of the relevant database, i.e. a backup where the database is shutdown until completion, is taken before major database or system upgrade.

Each week day media for the previous day's backup is removed for temporary offsite storage.

Backup Log

A daily backup log is issued to keep a report of backups, their status, which tapes are used and housekeeping of the backup system. These logs are stored in [specify location] and verify with designated member of staff.

Maximum Permissible Data Loss

1. In the event of a catastrophic machine loss or other disaster the maximum permissible data loss for production corporate applications data is 1 working day.

2. In the event of a single disk failure, the database should be recoverable to the last committed transaction.

3. In the event of a data corruption, the database or, if appropriate, the object(s) affected should be recoverable to a point in time prior to that corruption.
4. In the event of a database object, e.g. a table being deleted in error, the object should be recoverable to either the night before or the whole database to a point in time prior to the object being deleted.