TEXAS STATE UNIVERSITY
SAN MARCOS
The rising STAR of Texas

Server Backup and Recovery Guide

(January 13, 2010)

Backup copies of the operating system, application software, and critical data should be made on a regular basis. The frequency of backups, their retention period, and the method/media used may vary depending upon the criticality of the services available from the server.

1. Frequency: Backup frequency will depend on the volatility and criticality of the files being backed up and on the cost and time required to recover the lost files by other means. For example, operating system and application software files may not change very often (low volatility) and may be recoverable from their original media, whereas spreadsheet and database files may change daily (high volatility) and their original source data may be difficult to obtain.

   A current backup copy of the most recent version of the operating system and application software should always be available in case the server has to be rebuilt. These copies are generally obtained from the hardware/software vendor at the time of purchase or initial installation. Server administrators should create a new backup of the currently installed version of the software as soon as possible after the application of each software upgrade/update.

   Backup copies of the server resident data files should also be available in case the current data is lost. The frequency of the backups should consider how much time and effort the user would need, or can afford, to invest in manual recovery of lost transactions. An application with low activity and paper documents recording transactions may only need to be backed up occasionally, maybe weekly. An application database with a high volume of transactions and little paper documentation of these transactions requires daily backup.

2. Retention and Cycling of Media: Many different schemes exist for rotating and replacing the oldest backup with the most current. Some keep many copies of the data (up to a years worth), others just a few. The key factor in determining backup retention is how far back one is willing to go to recover lost data.

   One method is the "grandfather, father, son" method where three versions are kept, the oldest version is always replaced by the newest. This method allows restoring of data to a point from 48 to 72 hours prior, in the case of a daily backup cycle, or two to three weeks in the case of a weekly backup cycle.

Another method often used in daily backup schemes involves the designation of a different set of backup media for each day of the week. Monday's backup is retained until the following Monday, at which time it is overwritten. Tuesday's backup is retained until the following Tuesday when it is overwritten, and so on. In this scheme, Friday backups are often retained for longer periods (e.g., a month). Thus, the backup of the 1st Friday of the month is retained until the 1st Friday of the following month when it is overwritten. This method provides recovery to any day in the prior week and to a designated point in each week of the prior month.

There are numerous variations on the methods described above. Regardless of the method, procedures for generating backups should be written and all backup media should be clearly labeled. Obsolete backup media shall be destroyed as described in section 04.10 of UPPS 04.01.01, Security of Texas State Information Resources.

3. Offsite Storage: Once the frequency of the backups is determined, consideration should be given to storing some of these backups at an offsite location and not in the server room location along with the servers. Otherwise, the same disaster that destroys the server facility is likely to destroy the backups of what was on the server. For this reason, it is a common business best practice to have a copy of the software and data kept at an offsite location.

   There are different schemes used for rotating backups to offsite locations. It is always best to have the most current copy of the data stored offsite. Where this is impracticable, consider sending the most current copy offsite at least weekly or monthly. In the above example, where Friday backups are recycled monthly, the Friday backups are often taken offsite. If data were backed up daily and a copy sent offsite weekly, the worst-case scenario in the event of a disaster would be the loss of one weeks worth of data. Again, the criticality of the data should drive the decision.

   Ideally, the backup data that is rotated offsite should be stored in a location that is as physically secure as the onsite location, yet accessible during an emergency situation. Offsite backups should also be encrypted to reduce risk should they be lost in transit to/from the offsite location. One method that can be utilized is storing backups in another building on campus, perhaps using a reciprocal agreement with another server administrator. A locking fireproof file

cabinet, where you have control over the keys, is best. Keeping backups of university data at an employee's home is unacceptable. The employee could sever ties with the University and not return the data files. There is also no way to assure restricted access to the backup data when it is stored in someone's home.

4. Testing Recovery: One of the most important but often neglected steps is actual testing of all the plans and procedures in place to recover from a disaster. It can be time consuming and requires careful planning. However, the recovery of a complete system or selected applications from backups should be tested once or twice a year if possible. At a minimum, the data files should be restored periodically to make sure the backup generation process works correctly and the data is recoverable in a useable form. As processes change, the backup plan may need updates and the best way to determine this is through testing.