KILIMANJARO
CONSULTING

Kilimanjaro Consulting Pty Ltd

Backing up and recovering your data

Prepared by Kilimanjaro Consulting Pty Ltd | Revision V3, 2 July 2012

EXO
BUSINESS
MYOB ENTERPRISE SOLUTIONS

Level 4
122 Walker Street
North Sydney NSW
2055 Australia

Postal Address
PO Box 6482
North Sydney
NSW 2059 Australia

Tel (02) 8923 5555
Fax (02) 8904 0089
Support 1300 857 464
support@k-c.com.au

www.kilimanjaro-consulting.com.au
KILIMANJARO CONSULTING PTY LTD ABN 32 120 531 937

Backups

It is important to back up critical data in a way that allows it to be quickly restored in the event of data loss. Data loss may be a single corrupt file or all your data. Potential events that can result in data loss include:

- Hard disk subsystem failure.
- Power failure that results in corrupted data.
- Systems software failure.
- Accidental or malicious deletion or modification of data.
- A destructive virus.
- Natural disasters, such as fire, flood, or earthquake.
- Theft or sabotage.
- Mistakes made by your systems administrator.
- Upgrading your server and failing to copy across all relevant data

Your ability to recover quickly from any outage or disaster, from a component failure to the complete destruction of a site, directly contributes to your ability to survive the disruption. A backup and recovery process should be in place for all types of failure.

Responsible Persons:

Make a member of your team responsible for your backups, and make sure that it is being done every day. Check the backup register each week to track this. (See below).

Description

SQL Database Backup (SQL Server)

The backup of your data in the SQL database can be automated to make a copy of the EXO database to the hard drive on your server. This backup copy only protects you against a corruption in the live SQL database. If your server or hard drive is destroyed or has a catastrophic failure, you will not be able to recover either the live copy or this backup copy. It is however essential to have this copy as the most common problems in the SQL data can be easily recovered from this copy.

Check with your systems administrator if the SQL server backup has been configured. Ideally, this should scheduled to run every day, outside of normal working hours, and configured to keep the last 30 days of backups. On day 31, the system with automatically delete day 1, so you always have 30 days of backups.

If you are running more than one company on EXO, you will need to configure multiple backup schedules.

Server Backups

It is essential to have a copy of all files and programs that are saved or installed on your server.

Operating System and Programs

You should keep all the original installation disks of any software you purchase, as the programs will have to be re-installed from these disks in the event of a catastrophic server failure. You will also need to know where the licence "keys" or registration codes for the software are kept.

File server (Data files)

For your MYOB EXO programs implemented by Kilimanjaro (we have a standard folder structure) you will need to be sure the following folders are backed up:

Monthly or more frequently:

- EXO Folder

Weekly or more frequently:

- Clarity sub folders
- Documents sub folders
- GL_Reports sub folders
- Images sub folders
- Bank_Files sub folders
- Templates sub folders

Exchange Server

The Exchange Server manages your Microsoft Outlook (Emails, Calendar, and Tasks etc). It is essential to have this backed up daily. Make sure that your Network Administrator has configured your email so that in the event that your server is off-line, your emails get stored at your ISP and cascade down once your server comes back on-line.

Backup Exec Software (or similar)

Backups can be done manually on small sites, but on larger installations it is preferable to use a backup program such as Backup Exec to automate the backups.

The backup program can be set to run every day at (say) 3:00 am. The program backs up all data to the media (tape drive or removable hard drive).

Requirements

Tape, external hard drive or other media backups

You will need one tape, external hard drive or USB for each working day of the week, (so if you work 5 days a week, you need 5 tapes or 5 disks). This is called the daily backup, and you will re-use the Monday tape[1] each Monday, the Tuesday tape each Tuesday etc etc.

plus

One tape (or other media) for each week (5 tapes for a 5 week month). This is called the weekly backup. You will use the Week 1 tape each first week of the month, the Week 2 tape each second week of the month etc etc.

Plus

One tape (or other media) for each month you wish to keep. It is at your discretion how many months you keep. This is called the monthly backup.

In most cases, you would keep your financial year end backup tape (eg. Month tape for June) indefinitely. This would be your annual backup.

Procedure

Step One

Clearly mark all your tapes, as indicated above.

Step Two

Remove the current tape a put it back in its cover and then insert the next required tape. This could be either a daily, weekly, or monthly tape; consult the Tape Backup Check List sheets to see which tape to use next if you are unsure.

[Once completed, weekly and monthly tapes should be removed and stored off site.]

[1] Tape refers to any removable media, such as removable hard drive or USB Key

Step Three

Complete the Tape Backup Check List every day. See example below. Management should check to see that this is being completed.

Table 1: Sample Backup Register

Date	Tape	Name	Successful ?	Tested	Notes
21 July	Monday Tape				
22 July	Tuesday Tape				
23 July	Wed Tape				
24 July	Thurs =Weekly No.4				
25 July	Friday Tape				
26 July	Saturday – No activity so no backup required				
27 July	Sunday – No activity so no backup required				
28 July	Monday Tape again				
29 July	Tuesday Tape again				
30 July	Wed Tape again				
31 July	Thurs = Weekly No.5				
1 August	MONTHLY Tape 1				

Testing (To be completed by network administrator)

The Network administrator must ensure that the data on the tape or media is recoverable.

Backups should be periodically tested by restoring multiple files from the tape to an alternate location. If this operation succeeds put a tick in this box in the check list; otherwise put a cross.

Disaster Recovery

The network infrastructure within your company forms the basis for the operations of the company. It is therefore essential to prevent permanent loss of data and to minimise downtime. You should plan in advance for disaster recovery. The approximated downtime will only be achieved if you have made plans for disaster recovery. Without planning, your downtime may be days.

Cloud

Cloud based disaster recovery servers are becoming more common. Ask your Network Administrator for details

Virtualisation

Where servers are built in a virtual environment, recovery from disaster is much easier as an image of the entire operating system with software can be created. This image can then be transferred to another virtual server. Ask your Network Administrator for details

Disaster Scenarios

Hard Drive in the File Server fails

- Remove the damaged Hard Disk Drive and replace it with the new drive.
- Install Operating System from original disks
- Restore ALL data from last reliable Backup
- Install software Licences

Approximate Downtime: 2-4 hours

File Server Encounters a Physical Problem

The problem needs to be determined. Issues with cards, (video, network, etc) memory, or the power supply will require these devices to be replaced

Approximate Downtime: 2 hours

If the processor or motherboard is faulty, remove the server and replace it with a workstation and configure the workstation to be a temporary SBS Server. This will require the installation of CDROM, Tape Drive, SCSI Controller and the Hard Disk with the pre-configured operating System and Backup Software. Restore ALL data from the last reliable backup, and reinstall software licences.

Approximate Downtime: 2-4 hours

File Server is Stolen or Destroyed. (Fire, Flood, etc)

Replace the server with a workstation and configure the PC to be a temporary SBS Server. This will require the installation of CDROM, Tape Drive, SCSI Controller and the Hard Disk with the pre-configured operating System and Backup Software. Restore ALL data from the last reliable backup, and reinstall Software Licence.

Disaster Recovery Pack: (Located off-site)

Larger organisations may elect to have a disaster recovery pack off-site. This is often a fully configured server, which only requires the latest backup to be restored to it. It is essential that this server has the ability to "read" your backup tapes or other media. Cloud based disaster recovery servers are becoming more common.

Contents:

Tape Drive compatible with backup tapes

Tape Backup of the last Month

Microsoft Small Business Server + Recovery Disk

Windows Operating System Disks

Backup Exec CDROM

Software Licences (If required)

Spare hard drive