

Data Backup & Recovery Plan
Prerequisites, Backup Procedures and Recommendations

Table of Contents

Purpose	2
Prerequisites	2
Backup Hardware	2
Backup Software	2
Disaster Recovery Diskettes	2
Secure Onsite Location	2
Secure Offsite Location.....	2
Machine Configurations.....	2
Database Backups	3
Backup Procedures	3
Quarterly Backups.....	3
Monthly Backups	3
Daily Backups	3
General Principles	3
Disaster Recovery Diskette Renewal.....	4
Media Storage Procedures	4
General Storage Rules.....	4
Restore Procedures.....	4
Known Risks	5
Further recommendations	5

Data Backup & Recovery Plan

Prerequisites, Backup Procedures and Recommendations

Purpose

This document describes recommended guidelines for data backup procedures, media storage procedures, and data restore procedures for a small to medium size business. When properly implemented, this plan can provide reasonable insurance against loss of data. **Please be aware that no plan can guard against all contingencies.**

Prerequisites

Backup Hardware

The tape drive on the network should be of sufficient capacity to back up, with disaster-recovery capability, the entire contents of every server on the network.

Backup Software

We recommend the ArcServe backup package. While not inexpensive, ArcServe allows for centralization of the backup process and provides clients for Windows, Unix, and Novell systems. Centralization is important because it will reduce the time required to implement and verify the backup process and will provide an invaluable troubleshooting aid in the event of a backup failure.

Disaster Recovery Diskettes

A set of disaster recovery or “boot disks” should exist for each system. On Windows-based systems, these disks should contain the contents of the installed registry. On Unix systems, the disks should contain enough information to mount the existing filesystems as root.

Secure Onsite Location

An industrial-grade fire safe on the premises can serve as a secured onsite location, provided that the safe is kept locked at all times. An unlocked safe will not provide any protection in the event of a fire.

Secure Offsite Location

Your business should obtain access to a secured offsite location, such as a safety deposit box or similar infrastructure. In the event of an explosive attack or natural disaster, your onsite storage safe may not survive with its contents intact. The risk to stored media should be spread out to two physical locations.

Machine Configurations

Document the physical hardware in each server, and store a copy in both the onsite and the offsite locations. **Review the documentation quarterly** to ensure that it is kept current. The documentation should include:

- the physical build and interconnection of the systems
- the BIOS settings
- any RAID controller configuration

This information will be invaluable in the event of a hardware loss or failure.

Data Backup & Recovery Plan

Prerequisites, Backup Procedures and Recommendations

Database Backups

Set all database systems to back up the data to local disk-based device files in the hour prior to the beginning of the tape backups. This will insure that the database integrity is preserved in the backup process.

Backup Procedures

All backups should be full system backups. With the low price of storage devices and media, it is a much less complex problem to take full backups rather than incremental backups. It also reduces the time necessary to perform a full system restore.

Backup procedures will be discussed in order of increasing frequency of procedure:

Quarterly Backups

At the end of each quarter:

1. Take a full system backup of each computer, and store the backup at the offsite location.
2. Take a second backup to be stored onsite, to facilitate ease of recovery should it be needed.
3. Within 48 hours of taking this backup, restore the backup onto a testbed computer to verify proper operation.

Monthly Backups

On the last day of each month:

1. Take a full system backup, and store the backup at the offsite location
2. Verify backup within 48 hours

Daily Backups

Obtain enough backup tapes to keep two weeks worth of daily backups plus one “rover” tape (11 tapes per server). At the end of each business day:

1. Take a backup at the end of each business day
2. Store the current week’s set onsite
3. Store the previous week’s set offsite

On Monday evenings:

1. Insert the “rover” tape into the tape backup drive
2. Take the five tapes from the previous week to the offsite facility
3. Transfer the five tapes from the offsite facility to the onsite facility
4. Set aside the previous “Monday” tape to be the next week’s rover tape.

General Principles

Perform a **weekly spot-check of a random backup tape** by restoring it to a testbed computer. Rotate the server that the backup comes from to insure a good sampling. If a backup should fail or a tape should be flagged as faulty, immediately investigate and correct the underlying cause.

Data Backup & Recovery Plan

Prerequisites, Backup Procedures and Recommendations

Disaster Recovery Diskette Renewal

Every **30 days**, create a labeled and dated set of disaster recovery diskettes for each system. Store one set onsite and one set offsite. **After 6 months of storage, discard the media.** Any time that there is a modification to the installed software or hardware base, immediately create a new set of diskettes.

Media Storage Procedures

General Storage Rules

- Store tapes in a cool, dry environment. The tape's packaging will specify the environmental extremes that can be tolerated.
- Keep tapes away from monitors, speakers, and any equipment that emits a magnetic field. Magnetism will erase the tapes and diskettes.
- Tape sets should be given a number, and each tape in the set should be clearly labeled. The set should be stored in a container with a re-usable label. This label should be kept current with the date of the set.
- Do not handle tapes excessively. Avoid opening the protective doors on the tapes.
- Keep unused tapes in a locked container, and limit access to that container to key personnel.
- Keep the window of risk, during which all tapes are in one location, to a minimum. Tapes should move directly between the onsite and offsite locations.
- Do not leave the tapes unattended in a vehicle for any length of time, as it increases the likelihood of damage or theft.

Restore Procedures

Do not attempt restoration until the physical configuration of the hardware has been verified. The operator should check the system documentation and correct any differences found. If the original hardware is missing, the operator should procure an identical system where possible. In the event that an identical system is not available, the operator should endeavor to find one that is configured as closely as possible to the missing system. The most critical areas to address are the number of processors, installed device cards, and configuration of storage devices including RAID controllers.

Do not attempt to restore tapes onto hardware with a RAID level or storage configuration different from the system that the original backup tape and/or restore diskette were created from.

To restore a system, the operator should collect the following:

- the most recent backup tape
- the ArcServe install media
- the most recent disaster recovery diskettes for the system

Boot the recovery diskette #1 from the set, and follow the prompts to completely restore the system.

Data Backup & Recovery Plan

Prerequisites, Backup Procedures and Recommendations

In the event of a restore failure, the operator should work backwards in time from the current media. For example, if the tape fails to restore using the tape from Wednesday, the operator should re-try the operation using the Tuesday tape.

If the recovery diskettes fail to function, the operator should first retrieve the offsite copy of the diskettes and attempt to perform the restore procedure before moving to a previous date.

In the event of device failure during the restore the operator should replace the failed device and try the restore process again.

Known Risks

When closely followed, the procedures in this document will provide a high degree of availability, redundancy, and ease of system restore. However the following circumstances could result in partial or even full data loss:

- ***Complete failure of all magnetic media.*** This is statistically unlikely but could occur. Random spot-checks of the media integrity will mitigate this threat.
- ***Terrorism or Natural Disasters.*** In the event that both the onsite and offsite secure locations are damaged or destroyed, the integrity of the backup media may be questionable. Separating the two locations in both physical space and organizational control will mitigate this risk. In other words, keeping the media in a bank on the other side of town will be more secure than keeping the media in a branch office or in a nearby facility.
- ***Procedural breakdown.*** This is the most likely cause of failures and should be taken very seriously. In addition to implementing the prerequisites (with the exception of the offsite facility) and setting up a backup schedule to insure that the proper data is protected, it will be up to your staff to properly implement the changing of tapes and the storage of media.
- ***Normal data loss upon active restoration of data.*** Any restoration of data will lose any changes in the data that happened between the time of the backup and the time of the restore. Frequent backups will keep the maximum data loss to one to three days worth.

Further recommendations

- Invest in an auto-loader tape caddy, especially if the number of servers is increased substantially.
- Perform more frequent spot-checks of the backup tapes to further demonstrate reliability of the process.
- Keep an unused redundant system in an offsite location to mitigate the risk of equipment failure or loss.