ADG | ARCHITECTS DESIGN GROUP

ADG DATA BACKUP AND DISASTER RECOVERY
POLICY STATEMENT

1.0 Overview

This policy defines the backup policy for computers within ADG, which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server and the mail server.

2.0 Purpose

This policy is designed to protect ADG data to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Data can be destroyed by system malfunction or accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. The ongoing availability of ADG Project data is critical to the business continuity of ADG. In order to minimize any potential loss or corruption of this data, units responsible for providing and operating administrative applications need to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure.

3.0 Scope

This policy applies to all equipment and data owned and operated by ADG.

The following typical threat is assumed for the data backup policy as part of minimal baseline protection:

- Demagnetization of magnetic data media due to ageing or unsuitable environmental conditions (temperature, air moisture)
- Interference of magnetic data media by extraneous magnetic fields
- Destruction of data media by force majeure, e.g. fire or water
- Inadvertent deletion or overwriting of files
- Technical failure of storage device (head crash)
- Faulty data media
- Uncontrolled changes in stored data (loss of integrity)
- Deliberate deletion of files with computer viruses etc

4.0 Policy

1 Timing
Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

2 Tape Storage
There shall be a separate set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday. There shall be a separate set of tapes for each Thursday of the month such as Thursday1, Thursday2, etc. Backups performed on Thursdays shall be kept for one month and used again the next month on the applicable Thursday. Backups performed Monday through Friday except Thursday shall be kept for one week and used again the following appropriate day of the week.

3 Tape Drive Cleaning
Tape drives shall be cleaned monthly and the cleaning tape shall be changed yearly.

4 Monthly Backups
Every month a monthly backup tape shall be made using the oldest backup tape.

5 Age of tapes
The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than twenty-four months shall be discarded and replaced with new tapes.

6 Responsibility
The IT manager shall perform the regular backups, develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.
Data backup should have at least one primary person-in-charge and one substitute. Data backup is a critical security measure thus the relevant persons-in-charge should be committed in writing to adherence to the specific data backup policies and procedures.
All persons-in-charge of data backup should receive adequate training on the data backup process, data restoration process, media rotation, retention and storage. Regular refresher and adherence checking on data backup must be conducted.

7 Testing
The ability to restore data from backups shall be tested at least once per month.

8 Data Backed Up
Data to be backed up include the following information:

User data stored in the user's Document folder.
Xserve server system data
ADG Xserve RAID data
Mail server
Sage Accounts data

9 Tape Storage Locations
Offline tapes used for nightly backup shall be stored in a fireproof data safe. Weekly Thursday1, Thursday2 etc and Monthly tapes shall be stored off-site until required.

10 Documentation
Documentation is necessary for orderly and efficient data backup and restoration. The person-in-charge of backups is to complete the printed backup schedule checklist kept in the safe for each generated data backup.

ADG DATA BACKUP AND DISASTER RECOVERY
POLICY STATEMENT

5.0 Definitions

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

6.0 Consequence of Non-Compliance:

Non-compliance with this policy could severely impact the continuity of ADG as a company. By being exposed to permanent loss of data leading to loss of project information, staff records, research material etc.

7.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Ian Potts Dip Arch RIBA, Managing Director - ADG, March 2012