3.4 Backup And Restoration

On Friday night, the office catches fire and everything is destroyed. How much data will be lost?

3.4.1 Workstation

Policy All work related data in any computer must be stored in a central file server.

Standard All network computers shall have network directory mapped to the file server.

Procedure

(1) System Administrator creates a directory for each user in the file server.

(2) This directory has read/write permission for the user only

(3) Map this directory as X: drive on user's computer

Guidelines

(1) The definition of "work related data" and its level of importance to be stored in the file server is up to the discretion of the individual department. The work related data can include but not limited to:

a. Documents
b. Source code of In-house developed applications
c. Presentation / proposal
d. Letters
e. Email

(2) All work-related data are to be stored on the mapped directory.

(3) Any standalone computer, which holds important data, must have its own backup medium or means to copy the important data to the file server. (separate policy required)

3.4.2 Server

Policy All work-related data in all servers must be backed up.

Standard There must be two types of backup: Daily and Weekly. Daily backup (Differential or Full) must be done at suitable time giving minimum interruption to the operation of the department concerned. Full weekly backups must be done in two sets.

Procedure

(1) Use appropriate backup & restore software and hardware / backup device.

(2) Label all media properly with the following information:
   a. Media ID
   b. Volume no (x of y)
   c. Description of Content

(3) Perform backup with data verification.

(4) Log the following information:
   a. Department/Location
   b. Media ID
   c. Volume No (x of y)
   d. Description of content (or Data Code)
   e. Differential / Full
   f. Daily / Weekly
   g. Name of Backup Operator
   h. Start Date/Time
   i. Completion Date/Time
   j. Server Name
   k. Remarks

(5) Keep the daily backup on-site.

(6) Keep one copy of full weekly backup on-site for restoration and the other for off-site safe keeping.

Guidelines

(1) Department concerned must verify that their backup is restorable.

(2) It is up to the discretion of the individual department to determine the sufficient number of generations of backups for restoration of data integrity.
daily: keep 7 days.
weekly: keep 4 weeks.
monthly: =4th week. keep 12 sets.
yearly: =52nd week. keep 7 sets for 7 years.

(3) The use of backup media, such as handling of tapes and the times of use, must be in accordance to the guidelines provided by the manufacturer.

(4) Backup media include but not limited to the following:

a. Diskette
b. CDR / DVDR
c. Magnetic tapes (DAT / DLT)
d. Thumb drive
e. Hard Disk