INFORMATION SECURITY GUIDELINE

Backup

Introduction

1. This guideline is meant to provide guidance on performing backups of UBC Electronic Information at the departmental/faculty level if not using a storage service that already handles backups such as the Home Drive Storage service from UBC IT.
2. This guideline has been issued by the Chief Information Officer to supplement the Securing Computing and Mobile Storage Devices/Media standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Types of Backups

3. There are three types of backups:

Backup Type	Description	Pros and Cons
Full	Captures all files on the disk or within the folder selected for backup	Because all backed-up files are recorded to a single media or media set, locating a particular file is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.
Incremental	Captures files that were created or changed since the last backup, regardless of backup type	This offers more efficient use of storage media, and reduces backup times. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.
Differential	Captures files that were created or modified since the last full backup Therefore, if a file is changed after the previous full backup, a differential backup will save the file each time until the next full backup is completed.	This takes less time to complete than a full backup. Restoring from a differential backup may require less media than an incremental backup because only the full backup media and the last differential media would be needed. As a disadvantage, differential backups take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.

4. Where time permits, all backups should be full backups.

How to Perform Backups

5. Generally, all information on servers should be backed up at the end of each day.
6. Backup media should be rotated according to a set schedule and labeled appropriately, so that the proper media can be found when it is needed for a restore.
7. Media labels should also indicate the date that the media was placed in service, so it can be replaced when appropriate. Typically, the media should be replaced every 2 years.
8. Backups should ideally be in file formats that use open standards as opposed to proprietary formats.
9. One or more persons should be designated with the responsibility to ensure backups are completed successfully each morning.

How Often to Perform Backups

10. How often data is backed up is determined on how often the data changes. If the data changes daily, then daily backups should be performed. At a minimum, data should be backed up weekly.
11. One example of a backup schedule is the “grandfather-father-son” backup, which refers to a common rotation scheme for backup media. A simple schedule is listed below:

Frequency	Backup Type	Notes
Monthly	Full	Monthly backups provide the baseline to restore/recover data from and should be retained as per the data retention schedules of UBC.
Weekly	Full or Differential	Weekly backups provide an interim baseline. A minimum of 2 weeks’ worth of weekly backups should be maintained; 4 weeks is recommended. Full backups are recommended at this level but Differential can be performed if time or space constraints are a limiting factor.
Daily	Full, Incremental, or Differential	Generally, there should be enough media to maintain 2 weeks’ worth of daily backups.

Backup Restore Tests

12. While the backup process is important, it is just as critical to test that the backups can be successfully restored. This is especially important with tape media because tapes wear out and tape drives get dirty over time.
13. The following steps can be followed to perform a simple backup restore test:
    a. Identify one document folder on your drive and rename it. Do not delete it.
    b. Locate the most current backup media and insert it into the particular system.
    c. Load the restore software and identify the original renamed folder on your backup media. Use the software to restore the folder back to the drive.
    d. Count the files in the freshly restored folder and the renamed folder; these should match.
    e. Attempt to open a selection of the files to verify they are not corrupt.
    f. Consider using a file hashing program to compare the hash values for each folder; they should match.
14. Backup restore tests should be conducted at least quarterly.

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Securing Computing and Mobile Storage Devices/Media standard