Backup Management Guideline

Resource reference: **VPS-33-G01**
Status: Approved
Last revision: **2024-02-19**

Introduction

This guideline defines a standard for the backups of Concordia's electronic information.

Concordia's Chief Information Security Officer has issued this guideline under the authority of Policy Number: VPS-33 - Information Security Policy.

Questions about this guideline may be referred to: ciso@concordia.ca.

Context

This document has been developed to provide data backup guidelines to all members of the University community. The purpose is to clarify and improve Concordia's overall:

- Data Integrity and Availability: These guidelines aim to maintain data integrity and availability within the University's IT resources. By implementing effective backup practices, the University ensures that critical data remains accessible and uncorrupted.
- Compliance with Record Retention Requirements: The guidelines help adhere to record retention requirements. By retaining backups for a specified duration (usually no less than one year), the University complies with legal and regulatory obligations.
- Data Loss Prevention: Backups serve as a safety net against data loss. In the event of accidental deletion, hardware failure, or cyber incidents, having reliable backups allows the University to recover essential information without disruption.
- Data Restoration: When IT resources or business processes are disrupted (due to system failures, disasters, or other incidents), having proper backups facilitates efficient restoration. It minimizes downtime and ensures continuity.
- Backup Testing and Validation: Regularly testing and validating backups ensures that they meet the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). This validation process helps maintain confidence in the backup system.
- Responsibilities and Accountability: The guidelines apply to all Data Trustees, Data Stewards, IITS, all IT system administrators, and end-users managing data as per Concordia's Data Governance Framework.

These guidelines are essential for safeguarding data, maintaining operational continuity, and meeting legal obligations within the University community.

Backup Types

There are three main types of backups: Full backup, differential backup, and incremental backup.

Backup Type	Description
Full	Full backup: The most basic and comprehensive backup method, where all data is sent to another location.
Incremental	Incremental backup: A backup strategy that copies only the modified data since the last backup (whether it was a full backup or another incremental backup) Incremental backups optimize storage space and are efficient.
Differential	Differential backup: A differential backup strategy copies only the newly added and changed data since the last full backup. Differential backups ensure faster restores but require more storage than incremental

Backup Requirements

1. All data should be classified according to Concordia's data classification model and protected accordingly including backups.
2. Generally, all information on servers should be backed up minimally at the end of each day.
3. 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.

4. Backup media should be replaced every 2 years or according to manufacturer recommendations.
5. Backups should be in file formats that use open standards whenever possible.
6. Backup responsibility should be formally assigned to ensure backups are completed successfully at least each morning.
7. Backup frequency should be determined by how often the data changes. At a minimum, data should be backed up daily or weekly if there isn't many changes.

Example Backup Schedule

Grandfather-father-son backup (GFS) is a common rotation scheme for backup media in which there are three or more backup cycles, such as daily, weekly and monthly.

Frequency	Backup Type	Notes
Monthly	Full	▪ Monthly backups provide the baseline to restore/recover data from and should be retained as per Concordia's data retention schedules as listed in the Records Classification and Retention Plan (RCRP).
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.

Physical Storage Security and Encryption

Physical security is fundamental to the overall safeguarding of any IT infrastructure including backup media. Most software-based security controls can be compromised if an attacker gains access to the physical facility and equipment.

Encryption is extremely important and mandatory when data is classified as Class 3: Confidential or higher as it ensures that even if your backup media is lost or stolen, unauthorized individuals cannot misuse your information. It provides reliability, accuracy, and validity to your backups, ensuring that the data remains unaltered.

Backup Retention, Recovery Time Objective, and Testing

Backup retention refers to how long you keep backup copies of your data. All data should be retained as per Concordia's data retention schedules as listed in the Records Classification and Retention Plan (RCRP).

Recovery Time Objective (RTO) is the maximum acceptable downtime for a system or service after a failure occurs. It is very important to define the RTO as this will help prioritize recovery efforts and minimize service disruption. A well-defined RTO ensures timely recovery, reducing financial losses and reputational damage. Build your RTO by:

- Assessing Critical Systems: Identify which systems or applications are critical to your organization's operations.
- Setting Realistic RTOs: Balance the need for quick recovery with practical considerations (e.g., complexity, cost).
- Test Recovery Scenarios: Regularly simulate failures and measure actual recovery times against RTO targets.

Backup testing involves verifying the integrity and recoverability of backup data. This is critically important to:

- Avoid Data Corruption: Testing ensures that backups are not corrupted and can be successfully restored.
- Detect Issues Early: Identifying problems during testing allows corrective actions before a real disaster occurs.
- Build Confidence: Regular testing instills confidence that your backup strategy works as intended.

When testing your backups, be sure to always:

- Schedule Tests: Regularly schedule backup tests (full, incremental, and differential) to validate data integrity.
- Test Different Scenarios: Simulate various failure scenarios (hardware failure, accidental deletion) to assess recovery effectiveness.
- Document Results: Keep records of test outcomes and any necessary adjustments to improve backup processes.

Cloud backups and software as a service (SAAS) providers

Backing up your data in the cloud or when using software as a service is a critically important aspect to consider and understand. IITS provides assistance and expert advice to help community members backup their data and align to best practices. The IITS Operations team is available by email at iits.operations@concordia.ca.

How to get help backing up your data

IITS provides assistance and expert advice to help community members backup their data and align to best practices. The IITS Operations team is available by email at iits.operations@concordia.ca.

Accessibility

Community members with accessibility questions or needs related to this guideline are asked to contact the appropriate IITS resource person by emailing iits-accessibility@concordia.ca.

Implementation, audit, and review

Concordia's Chief Information Security Officer (CISO) is responsible for the implementation, review, and approval of this guideline. Concordia's CISO initiates a review as often as necessary, but at least annually, to ensure alignment with both internal and external requirements and regulations.