IT Services

IT Services Backup Policy

Table of Contents

1 Revision History and Reference Documentation

Each time a new version of this document is released it should be recorded here.

Version	Date	Author	Comments
0.1	May 12th 2020	Patrick O'Regan	Initial version
0.2	Aug. 5th 2020	Infrastructure peer-review	Team comments incorporated
0.3	Sept. 17th 2020	HEAnet review	HEAnet review comments included
0.4	Nov. 5th 2020	Peter Gaughran	Added definitions
0.5	Nov. 8th 2020	Peter Gaughran & Patrick O'Regan	Review and Finalise
1.0	Nov 20th 2020	D O'Reilly	Reviewed & Approved
2.0	Jan 25th 2022 Jan 27th 2022	Data Centre Project Delivery Team (Jason Doran, Peter Gaughran, James Burke, Stephen Power, Charlene McGoohan) Dearbhla O'Reilly HEAnet Security Services Steering Committee	Linked documents updated. Following sections have been added: Data Backup for M365 Data Data Backup for Azure Data Centre Third Parties Approved
Review:	Q3 2023		

Reference Documentation
IT Services Backup Procedures – Netbackup
Netbackup Schedules
MU Resiliency Assessment (IBM) approved ITMSC April 2018
SAN failover Recovery (pptx)
MU Major Emergency and Critical Response Plan
IT Services DR Plan Test Schedule
IT Services Major Incident & Communications Plan 2017

2 Introduction

Information Technology systems and services play a major role in supporting the day-to-day activities of the University and in delivering many important services to the Maynooth University user community. It is essential that these resources are protected to ensure the confidentiality, integrity, and availability of the information that they hold.

The objective of this backup policy is to describe how Maynooth University aim to safeguard the universities' information assets by ensuring that adequate back up controls are in place.

This will yield the following benefits:

- Clarify the backup requirements. Back up requirements are based on the criticality of the system, the agreed upon recovery point and recovery time objectives (RPO & RTO) and will be in line with MU's data electronic retention periods and legal requirements.
- Clarify the different means of backup (snapshot, installed client and database agent.)

2.1 Scope of this document

This document describes the data backup policy for systems and services managed and delivered by IT Services.
Any service specifically mentioned in IT Services Disaster Recovery Plan will be backed up as per procedure.

2.2 Exclusions

Any on-campus non-IT Services ICT infrastructure that **does not** impact the core services offered by IT Services (such as private compute clusters owned and managed by departments – Mathematics and Statistics, Theoretical Physics, Electronic Engineering, Computer Science, Hamilton Institute) are **not** covered by this document. Responsibility for the operation of such infrastructure both in day to day and post crisis mode reside with the local infrastructure owners.

2.3 Definitions

Back Up - a copy of a file, server or other item of data made in case the original is lost or damaged.
Restore - return a file, server or other item of data to a former condition, place, or position.
Recovery Time Objective - A metric that helps to calculate how quickly IT infrastructure/services needs to be recovered following a disaster in order to maintain business continuity.
Recovery Point Objective - A measurement of the maximum tolerable amount of data that can be lost. Useful for determining how often to perform data backups.

Service Owner - A role responsible for managing one or more services throughout their entire lifecycle.
Snapshot - A type of backup copy used to create the entire architectural instance/copy of an application, disk or system. It is used in backup processes to restore the system or disk of a particular device at a specific time.
Recovery Services Vault - An entity in Azure Data Centre that stores the backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

3 Data Backup Roles & Responsibilities

IT Services

Responsible for the implementation of this policy and other relevant policies within the IT Services area and for ensuring that there are adequate procedures and technology are in place to support the policy.

Service Owners

Responsible for the ownership, control, security and management of their data and also for ensuring that adequate backup procedures are in place (including Disaster Recovery and Business Continuity)

4 Data Backup Schedules & Means for IT Systems and Services

The storage infrastructure in the MU data centre supports the following backup options.

Backup Frequency

- Daily
- Weekly
- Monthly
- Before and after any major change to a system or application
- Adhoc – requested by data owner

Back up Type

- SAN Snapshot
- Installed client
- Database agent

Electronic data retention period for each back up type i.e.

- 1 month
- 3 months
- 6 months
- 1 year

5 Data Backup for M365 Data

Email Backup

Exchange Online mailboxes are continuously replicated to multiple database copies, in geographically dispersed Microsoft data centres, to provide data restoration capability in the event of a local messaging infrastructure failure.

Email Recovery

Deleted items are stored in the Deleted Items folder of the mailbox. Items removed from the Deleted Items are recoverable when dealt with promptly. If an item is deleted permanently, it is retrievable 14 days after deletion.

After the expiration or removal of a Microsoft 365 or Office 365 license, data is not instantly removed. The retention time is 30 days; this means that there is a period of 30 days before the data is entirely removed from Microsoft 365 or Office 365.

SharePoint/Teams/OneDrive Backup and Recovery

SharePoint Online and OneDrive for Business offer data retention based on the Recycle Bin functionality. Two levels of the Recycle Bin allow deleted files to be restored up to 90 days after deletion.

The first recycle bin retains data for 30 days. After this time deleted data is moved to the Secondary Recycle Bin where it is stored for an additional 60 days. After this time data is permanently deleted.

There is an additional 14 days to restore deleted files based on a service request sent by IT Services to the Microsoft Service team.

6 Data Backup for Azure Data Centre

A Recovery Services vault is an entity that stores the backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines. Azure Backup automatically handles storage for the vault.

Backup Frequency:

- Daily

Instant Restore:

- Retain instant recovery snapshot(s) for 2 days

Retention of daily backup point:

- Retain backup taken daily for 30 days

7 Third Parties

Where IT Services are the service owners/contract managers for third party managed services, IT Services will ensure that the third party is providing a secure backup solution where the minimum requirements meet the backup model outlined in this policy. Exceptions to this need to be formally justified.

8 Policy Review

This policy will be reviewed bi-annually (2 years) or after significant change to the MU infrastructure.