Standard: Backup and Recovery Standard

Effective Date:	2017.10.01
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Director, Information Security and Compliance
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

All electronic information considered of institutional value should be copied onto secure storage media on a regular basis (i.e., backed up), for disaster recovery and business resumption. This standard outlines the minimum requirements for the creation and retention of backups. Special backup needs, identified through technical risk analysis that exceeds these requirements, should be accommodated on an individual basis.

Who/what does the standard apply?

Data custodians are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. Backup provisions allow business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of institutional data backups need to be maintained.

Definitions

- **Restricted Data:** Information that is highly sensitive both externally and internally at the University. Unauthorized access could reasonably be expected to cause serious harm to individuals, businesses, other third parties or the University.
- **Protected Data:** Information that is sensitive externally and may be somewhat sensitive internally at the University. The inappropriate release of the Information would reasonably be expected to cause minimal to moderate harm to individuals, businesses, other third parties or the University.
- **Public Data:** Information that is intended for or is available to the public.
- **Data Owners:** Data Owners are the unit managers, members of the top management team, or their delegates who bear responsibility for the acquisition, development, and maintenance of production applications that process University information.
- **Data Custodians:** are in physical or logical possession of either University information or information that has been entrusted to University of Manitoba. Custodians are responsible for safeguarding the information and making backups so that critical information is not lost.

Compliance

Data custodians must align to the requirements and specifications outlined within this standard. Where a custodian is unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

General Specifications

Requirement	Specifications
Backup Media	Backups must be regularly tested as determined by a risk assessment or at a minimum on an annual basis to ensure data can be restored in case of a catastrophic event. Backup media must be stored and transported in an appropriate, safe and secure manner and access to backup media must be restricted to only authorized personnel.
Off-Site Storage	Backup media stored off site must be stored in a secure location with environmental controls and appropriate access controls commensurate with the security requirements and criticality of the information stored in the backup. The current location is a third party secure warehouse in Winnipeg.
Backup Media Disposal	Obsolete backup media must be disposed of in a safe and secure manner, in accordance with University Data Destruction Standard. Backup media to be disposed of must be rendered unreadable through an appropriate means and an audit trail of disposal of backup media must be maintained.

Specifications: Standard UofM IT Service (Production and Test) Service: CommVault

Requirement	Specifications
Daily Backups	Daily Incremental backups performed every weeknight and stored for a minimum of 30 days on de-duplicated disk.
Monthly Full Backups	Performed on the middle of the month, stored on-site for 12 months (LTO5 Tape)
Weekly Disaster Recovery Full Backups	Performed weekly, stored off-site for 21 days in a 3 week cycle (LTO5 Tape).

Specifications: Disaster Recovery Backup Services for High Volume, Low Rate-of-Change Data Service: CommVault

Requirement	Specifications
Base Full Backup	Base Full taken as “Seed” and stored off-site. (LTO4 Tape)
Incremental Backups	Incremental Backups based on the “Seed” taken weekly and retained off-site indefinitely. (LTO4 Tape)
Periodic Refresh of Base Full “Seed”	As time permits.

Specifications: NCTR Vault Data Service: CommVault

Requirement	Specifications
Base Full Backup	Base Full taken as “Seed” and stored off-site. (LTO4 Tape)
Incremental Backups	Incremental Backups based on the “Seed” taken weekly and retained off-site indefinitely. (LTO4 Tape)
Periodic Refresh of Base Full “Seed”	As time permits.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Data Security Classification Guideline	