Long Term Storage of Information Standard

Section 1 - Purpose

(1) Information is one of RMIT's most valuable assets. It must remain accessible, protected and trustworthy for as long as legally required.

(2) RMIT must comply with Public Records Office Victoria (PROV) standards issued under the Public Records Act 1973. These standards specify how the information we create as part of our work – or records - must be managed.

(3) This standard must be used to manage data and information when it needs to be moved from an active, high availability location to a less active, medium/low availability location/s.

Section 2 - Authority

(4) Authority for this document is established by the Information Governance Policy.

Section 3 - Scope

(5) This standard applies to any person or entity of the RMIT Group, including staff, students, temporary employees, contractors, visitors and third parties who manage RMIT information in line with the Information Governance Policy.

(6) This Standard applies in any situation where RMIT data and information is being stored and may include (but is not limited to) on-site, RMIT controlled offsite, third party managed or any other storage location.

Section 4 - Standard

Movement and Storage Requirements

(7) The movement and storage of data and information must support the retention of data and information for as long as it is required for legal and business purposes, including for data analytics purposes.

a. Selection of storage locations must be informed by retention requirements, including the ability to apply legal retention periods as per the Retention and Disposal Standard and the longevity of the location/platform.

(8) The movement and storage of data and information must provide sufficient protection over time.

a. Data and information must be protected from misuse, loss, deterioration or damage and inherit or have appropriate information security classifications applied as per the Information Governance Policy.

(9) The movement and storage of data and information
must support timely discovery and access, by supporting the application of appropriate metadata.

(10) Ownership and accountability for data and information remains with the Information Trustee across its lifecycle, regardless of age or location.

(11) Information in long term storage must have an appropriate disaster recovery and business resilience plan in place.

Format

(12) Data and information should be stored in technology-neutral, sustainable formats wherever possible, and in accordance with PROS 19/05 S3: Long Term Sustainable Formats.

Copies

(13) Data and information required for long periods must be stored in locations that conform to this Standard and all other Information Governance and ITS resources. The following represent principles should be considered for storage systems:

a. Redundancy and diversity
   Make multiple independent copies of digital material, using different storage media, and store these in different geographic locations.
b. Fixity, monitoring, repair
   Use fixity measures such as checksums to record and regularly monitor the integrity of each copy of the digital material, using alternate copies to repair corruption/loss if required.
c. Technology and vendor watch, risk assessment, and proactive migrations
   Understand that storage technologies, products and services all have a short lifetime; be proactive in migrating storage before digital material becomes at risk
d. Consolidation, simplicity, documentation, provenance and audit trails
   Minimise the proliferation of legacy media types and storage systems used for preservation; document how digital materials have been acquired and transferred into the storage systems as well as how the storage systems are set-up and operated and use this to provide audit information on data authenticity.

(14) A copy of data and information created for back–up must not be used as a long-term storage solution.

Export

(15) An export function must allow timely, cost efficient and complete extraction of all information, data and metadata in technology-neutral, sustainable formats wherever possible.

Status and Details

Status	Historic
Effective Date	11th August 2021
Review Date	11th August 2023
Approval Authority	Chief Data and Analytics Officer
Approval Date	10th August 2021
Expiry Date	18th November 2023
Policy Owner	Nonna Milmeister Chief Data and Analytics Officer
Policy Author	Henrique Delamanha Mendonca Director, Data Management and Governance
Enquiries Contact	Data Management and Governance

Glossary Terms and Definitions

"**RMIT Group**" - The University, its controlled entities and strategic investment vehicles (known as the RMIT Group).