Information Technology Services Operations Manual - Master Data Management, Data Classification and Usage, and Data Storage

Policy code:	OG2083
Policy owner:	Director, ITS
Approval authority:	Chief Operating Officer
Approval date:	05 March 2024
Next review date:	18 August 2024

Table of Contents

1. Introduction

The Information Technology Services procedural manuals detail the processes that have been developed using previous policies, procedures to provide clear advice to Federation University Staff regarding their responsibilities, actions and accountability in accordance with the Federation University Act, Statute, Regulations and Policies Procedures and Manuals.

It is an associated document within the Federation Governance document suite and must be used as a tool to assist all stakeholders to fulfil obligations in accordance with university mandates.

The purpose of this manual is to ensure that all members of the Federation community are informed, understand their requirements to perform key tasks and know where to access information as needed to adhere to mandated requirements and enhance their practice.

It is also intended to assist all staff in carrying out their functions and responsibilities with ease and completeness by providing clarity of expectation and responsibilities.

This manual will be revised annually by the owner and/or their nominated delegates to ensure currency of information.

2. Master Data Management

2.1 Purpose

Federation University Australia is committed to the appropriate storage of information in support of its teaching, administrative and support functions. The University acknowledges its obligation to ensure appropriate security of personal data in relation to all relevant legislation while providing approved data storage solutions to accommodate the varying needs of the University community. University data is recognised as a valuable asset and will be efficiently managed and availed through development of a best practice approach to data management.

This procedure mandates a range of associated University policies and procedures developed to ensure the integrity, authenticity, availability, access, confidentiality and security of data produced and/or utilised by the University through minimising duplication and fragmentation and introducing internal controls to mitigate identified risks.

Through its associated procedures the University will:

- define the roles, responsibilities and accountability for different data usage
- ensure best practice processes for effective data management including access, retrieval, reporting, managing and storing
- protect the University's data against internal and external threats.

The University is also required to produce evidence of its activities to external regulators, internal auditors, accreditation and funding bodies. Adherence to this procedure will ensure the University is able to meet this requirement.

The University's *Research Data Management Policy* and *Research Data Management Procedure* (in draft) governs responsibilities and processes for the ownership, storage, retention, accessibility for use and reuse and/or disposal of research data in accordance with the Australian Code for the Responsible Conduct of Research.

2.2 Scope

This procedure applies to all University data produced, collected, stored and/or utilised by members of the University's community. It does not apply to data used for the purpose of academic research.

While partner provider organisations are supported through the use of specific University information technology systems, this procedure does not apply to non-University related data created, managed or stored by these organisations.

2.3 Legislative Context

The following categories of people are permitted access to the computing and communication facilities:

- Federation University Australia Act 2010
- The Higher Education Support Act 2003
- The National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students made under the Education Services for Overseas Students Act 2000 (ESOS)
- Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- Information Privacy Act 2000 (Victoria)
- Electronic Transactions Act 2000 (Victoria)
- Public Record Act 1973 (Victoria)
- Australian Copyright Act of 1968
- Evidence Act 1958 (Victoria)
- Australian Code for the Responsible Conduct of Research (2007)
- OECD Principles and Guidelines for Access to Research Data from Public Funding (2007)
- Australian Qualifications Framework AQF Second Edition January 2013
- Australian Skills Quality Authority ASQA
- Higher Education Standards Framework (Threshold Standards) 2011
- Tertiary Education Quality and Standards Agency (TEQSA)
- Higher Education and Skills Group HESG
  - 2014 – 2016 VET Funding Contract

2.4 Definitions

Term	Definition
Authorised person	An individual or group of people who have been authorised to use and/or store data on the University's approved data storage system/s
Copyright	Intellectual property right that protects a body of work, not for ideas or information, but for the form in which they are expressed, from unauthorised use and is applied automatically when a work is created without the need to register or comply with formalities
Data	Data and records collected, created and/or maintained by the University including digital and non-digital information which can generally be assigned to one of the four data categories of public, general internal, protected or restricted
Data dictionary	Centralised repository of information about data such as meaning, relationships to other data, origin, usage and format
Data management	Defines the access rights, roles and responsibilities in relation to the management and protection of University data
Data integrity	Data accuracy and consistency over its entire lifecycle
Data owner	An individual or group of people accountable for specific data that is created, transmitted, used and stored on a system within the University

Data quality	Data currency, validity and relevance
School	Federation University Australia has a number of Academic Organisational Units
Intellectual property (IP)(including patents and trademarks)	IP is the application of the mind to develop something new or original, existing in various forms – a new invention, brand, design or artistic creation A patent is a legally enforceable right that is granted for any device, substance, method or process that is new, inventive and useful A registered trade mark is a legally enforceable right that is granted for a letter, number, work, phrase, sound, smell, shape, logo, picture and/or aspect of packaging
Metadata	Describes information about data, such that data can be discovered, understood, re-used and integrated with other data; information described in a metadata record includes where and when the data was collected, created, organised, transmitted (where applicable) and last updated and who is responsible, allowing correct attribution to the creators of the work
Record	Any record that is created or received by the University in the transaction of its business functions or resulting from research activities and retained as evidence of that activity which can include, but is not limited to, hard copy documents, electronic or digital records including email and information maintained as part of a database or business information system
Scholarly works	Any article, book, musical composition, creative writing or like publication or any digital or electronic version of these works that contains material written by academic staff or student based on that person's scholarship, learning or research but does not include work that is teaching material
Security	Safety of University data in relation to access control, authentication, effective incident detection, reporting and solution, physical and virtual security, change management and version control
University data	All data owned or licensed by the University
Users	Persons who use information resources and have responsibility for ensuring that such data is used properly in compliance with this procedure

2.5 Procedure Statement

This procedure provides the following set of guiding principles to maximise the University's data management capabilities to manage the needs of students, staff and other members of the University's community who create, receive, store, access, transmit, use, or dispose of data as part of their relationship to the University noting that both the types of data and requirements will differ:

Principle	**Demonstrated By:**
Any record generated as a result of University activities is an official	• Utilising secure and reliable storage platform/s to manage data centrally – refer Section 4: Data Storage; data stored on local PCs and laptops is

record under the Public Records Act 1973 (Victoria) and must be created, captured, stored and effectively managed within the University's approved data storage and records management systems	the responsibility of the user and should be transferred to University's sanctioned storage • Capturing the activities and functions of the University to adequately represent institutional memory
The University's data classification scheme standardises records' structures and descriptions by contextualising the records within functions and activities	• Classifying data utilising the University's information security classification so that it may be managed and secured in a manner appropriate with its sensitivity and importance - refer Section 4: Data Storage • Categorising and using files consistently within the established classification scheme – refer Section 3: Data Classification and Usage
The University protects the confidentiality of personal and health information it collects for both its own operations and the conduct of research	• Complying with the University's *Information Privacy Policy* and *Student Access, Progression and Wellbeing Policy* • Ensuring that all personal and health data is stored in accordance with the Australian Privacy Principles, Ethical Conduct and other standards related to health records, as appropriate • Storing completed participant consent forms required in the conduct of researchprojects, clinical trials or other approved University activities eg Open Days in accordance with National Guidelines and Standards
Ownership and rights associated with data created, collected and stored is clarified and managed appropriately	• Facilitating appropriate management of all data created or collected • Determining inclusion of appropriate/sufficient details to ensure storage and access to records in accordance with any contractual agreements or sponsorship • Ensuring that scholarly works and data created by staff or students is owned by their creator/s unless the status is otherwise altered giving intellectual property rights to the University
The legal context for the collection, management, storage and use of data is considered and addressed	• Identifying data which is likely to pose legal issues to ensure storage and access options are suitably managed • Ensuring that any legal issues relevant to the collection, management and storage of data are addressed
Extensive metadata is built around the data to ensure quality information about its provenance, legal and technical framework, access rights, publication and disposal in line with relevant metadata standards	• Collecting and publishing metadata related to the data • Keeping good records and contextual information to ensure data is easy to locate and accessible into the future • Incorporating structured metadata eg properties which include title, author, subject, keywords, version control information, dates and additional comments within agreed standardised vocabularies and ontologies
Long term storage, archiving and disposal requirements are identified and implemented	• Managing appropriately the transition of data along the curation continuum eg private to public domain • Considering and implementing solutions for storing and accessing ethnographic data, including language recordings • Retaining data in compliance with minimum regulatory or funding retention periods eg five years to perpetuity and within legal and ethical requirements

	• Disposing of data in an appropriate manner in accordance with the University's *Records Management Procedure*
Data disaster recovery and activity continuity planning is in place	• Ensuring each organisational unit has created and continues to maintain a current business continuity plan • Backing up on premise and cloud storage data in accordance with the defined schedules and server cloud agreements • Ensuring adequate measures are in place to prepare for and manage in the event of a disaster or disruption to facilitate the resumption of University activities and minimise threats to the University's information assets

3. Data Classification and Usage

3.1 Purpose

Federation University Australia recognises that its corporate and research data are important strategic assets. This procedure supports and mandates the implementation of Section 2: Master Data Management and *Research Data Management Procedure*. It expands on the principles outlined in these policies and provides direction and guidance on assessing the sensitivity and importance of University data and it's usage.

All University data created must be allocated a classification so that it is managed, used and secured in a manner appropriate to its importance and sensitivity.

3.2 Scope

This procedure applies to all digital and digitised data produced, stored and/or utilised by members of the University's community. While partner provider organisations are supported through the use of specific University information technology systems, this procedure does not apply to other non-University electronic data created, managed or stored by these organisations.

3.3 Legislative Context

- Federation University Australia Act 2010
- Information Privacy Act 2000 (Victoria)
- Electronic Transactions Act 2000 (Victoria)
- Public Record Act 1973 (Victoria)
- Privacy and Data Protection Act 2014
- Australian Copyright Act of 1968
- Evidence Act 1958 (Victoria)
- Australian Code for the Responsible Conduct of Research (2007)
- OECD Principles and Guidelines for Access to Research Data from Public Funding (2007)
- Australian Skills Quality Authority ASQA
- Higher Education Standards Framework (Threshold Standards) 2011
- Tertiary Education Quality and Standards Agency (TEQSA)

3.4 Definitions

A complete list of definitions relevant to this procedure is contained within Section 2: Master Data Management.

A further list of definitions **specifically** relevant to this procedure is included below:

Term	Definition
Data classification	A scheme comprising of four levels including Public, General Internal, Protected or Restricted The creator of University data is required to assess the importance and sensitivity of the data and assign a label to that data so that it can be managed and stored with the appropriate consideration
Data Steward	Entity that can authorise or deny access to certain data and is responsible for its accuracy, integrity and timeliness
Data user	Controls the collection, classification, processing, use or storage of specific data following specified protocols
General Internal Data	University data that is not generally made publicly available and release of such information may cause minor impact on the reputation of the University, other organisation or individual e.g. academic lecture notes
Information assets	Definable pieces of information in any form, recorded or stored on any media that is recognised as valuable to the University
Personal use	All non-work or study related use including internet usage and private emails
Metadata	Describes information about data, such that data can be discovered, understood, re-used and integrated with other data; information described in a metadata record includes where and when the data was collected, created, organised, transmitted (where applicable) and last updated and who is responsible, allowing correct attribution to the creators of the work
Protected Data	Confidential University data with limited access with unauthorised disclosure, modification; data that includes personally identifiable information, is commercially sensitive e.g. salary information, contracts, medical/health records etc and if released could cause reputational harm or embarrassment to the University e.g. budget data, academic records, student grades, planning or purchasing documents
Public Data	Data created with the intention of being in the public domain, that is publicly available and unlikely to impact on the reputation of the University, other organisation or individual e.g. academic calendar, unit outlines
Restricted Data	Strictly confidential or sensitive University information e.g. budget data, academic records, student grades, planning or purchasing documents, restricted to individuals who are explicitly granted access with unauthorised disclosure, modification or destruction and if released is most likely to cause reputational harm or embarrassment to the University, other organisation or individual, compromise Australia's national security, national interests, economy, stability, integrity or damage international

	relations or defence e.g. research requiring ethics clearances, information relating to allegations of fraud

3.5 Actions

3.5.1 Ensuring all University data is classified

	Activity	Responsibility	Steps
A.	Protecting data assets	Data Steward	1. Classify all data created commensurate with its sensitivity and value to ensure appropriate protection throughout its lifecycle e.g. creation/modification/ destruction 2. Ensure data is used only for the purposes as determined by its classification, relevant University policies, procedures and/or applicable legislation

3.5.2 Assigning data classification

	Activity	Responsibility	Steps
A.	Identifying the appropriate data classification	Data Steward	1. Utilise Appendix 1 - Data Classification Scheme to determine the correct data classification 2. Assign correct data classification on saving or completing the document or work 3. Ensure all required metadata fields are completed
B.	Reclassifying data	Data users	1. Ensure that the correct data classification is used for data created 2. Ensure that any required re-classification of data follows the correct Data Classification Scheme • NOTE: This step is important when dealing with data that falls into the Protected or Restricted classification

			3. Ensure all required metadata fields are completed
C.	Classifying data from another source	Data users	1. Ensure that data received from another source is classified to correctly match the University's requirements • NOTE: In some instances, the data may have an existing classification from its place of origin 2. Ensure all required metadata fields are completed

3.5.3 Allocating responsibilities

	Activity	Responsibility	Steps
A.	Ensuring correct access	Data Steward	1. Refer to Appendix 2 - Responsibilities Table and allocate access classification
B.	Storing data	Data Steward	1. Follow Actions within Section 4: Data Storage
C.	Disposing of data	Data Steward	1. Ensure all required approvals are obtained prior to undertaking any data disposal 2. Follow all data disposal requirements detailed within the University's *Records Management Procedure* and consistent with ethics requirements for research data

3.5.4 Changing or downgrading classifications

	Activity	Responsibility	Steps
A.	Reclassifying data	Data Steward	1. Downgrade when protection is no longer necessary/needed at the original level 2. Review when the data becomes inactive or no longer in regular use 3. Refer to Appendix 2 - Responsibilities Table and determine new classification to reflect changes in the

			data's criticality, confidentiality or sensitivity 4. Obtain approval from PrivacyOfficer to change, downgrade or dispose of data with Protected or Restricted classification 5. Follow correct records management disposal process when disposing of any electronic data – refer *Records Management Procedure*

3.5.5 Disclosing, transmitting and/or exchanging data

	Activity	Responsibility	Steps
A.	Approving data dispersal	Data Steward	1. Distribute, transmit and/or exchange data if/as required for a valid business need 2. Contact ITS and complete a Functional Design Document (FDD) 3. Follow FDD workflow approval process to transfer data between systems 4. Provide written approval for protected or restricted information to be transferred or processed on any third-party systems

3.5.6 Using data

	Activity	Responsibility	Steps
A.	Ensuring data usage is appropriate	Data Steward	1. Access and use data in accordance with the Data Classification Scheme and Level of Impact table 2. Ensure any data exchange is carried out with appropriate approvals – refer *Information Privacy Procedure* 3. Access the appropriate University's data storage option:

			• Business Systems The University's business systems store data that relates to a specific business function (i.e. student data is stored in the Student Management System) • SharePoint Access/store other types of data, excluding data that is classified as restricted • Cloud Any data stored/ accessed must comply with all legislative requirements and be fit for purpose e.g. classified as public

3.6 Records Management

Document Title	Location	Responsible Officer	Minimum Retention Period
Functional Design Document	The University's approved records management system	Information Technology Services	7 years after administrative use has concluded
Information Model (identifies relationships between major data entities and systems of record)	The University's approved records management system	Information Technology Services	7 years after administrative use has concluded
Migration plans and quality assurance checks for migrated data	The University's approved records management system	Information Technology Services	1 year after migration has been completed
System testing strategies, result forms and test reports	The University's approved records management system	Information Technology Services	7 years after administrative use has concluded

3.7 Appendix 1

3.7.1 Data Classification Scheme

Classification	Examples	Potential Impact (refer Level of Impact Table)
Public	Newsletter, education material created for public use, unit schedule, unit	Negligible adverse impact to the University if disclosed

	catalogue, campus brochure, campus map, annual report, published journal article	
General Internal	Academic lecture notes, unit content distributed via sanctioned learning management systems	May cause minor impact on the reputation of the University, other organisation or individual
Protected	Intellectual property, commercially sensitive research, personally identifiable sensitive information, credit/debit card details, disciplinary information, salary information, examination papers, binding contracts, HR personal evaluations, medical / health records Budget and financial data, de-identified clinical research information, curated data from research projects, audit reports, student academic records, student grades, strategy and planning documents, purchasing data	Would cause exceptional damage to the University, staff or students if disclosed These records manage University functions or business activities where greater restrictions are required to protect the rights and interests of both the University and individuals, or to limit the University's liabilities
Restricted	Confidential out-of-court settlements, records affecting national security, protected disclosures, security vulnerabilities	Could cause physical harm to individuals or impact the University's existence if disclosed These records manage University functions or business activities where wider dissemination would expose the University or individuals to significant risks or liabilities

3.7.2 Level of Impact Table

The goal of data security is to protect the confidentiality, integrity and availability of data assets. Data Classification reflects the level of impact to the University if confidentiality, integrity or availability of data is compromised:

	Potential Impact		
Security objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorised restrictions on data access and disclosure, including the means for protecting personal privacy and propriety information	The unauthorised disclosure of data could be expected to have a limited adverse effect on the University's operations, assets or individuals	The unauthorised disclosure of data could be expected to have a serious adverse effect on the University operations, assets or individuals	The unauthorised disclosure of data could be expected to have a severe or catastrophic adverse effect on the University operations, assets or individuals
Integrity	The unauthorised disclosure of data could be expected to	The unauthorised disclosure of data could be expected to	The unauthorised disclosure of data could be expected to have a severe or catastrophic

Guarding against improper data modification or destruction and includes ensuring data non-repudiation and authenticity	have a limited adverse effect on the University's operations, assets or individuals	have a serious adverse effect on the University operations, assets or individuals	adverse effect on the University operations, assets or individuals
Availability Ensuring timely and reliable access to and use of data	The disruption of access to or use of data or a data system could be expected to have a limited adverse effect on the University's operations, assets or individuals	The disruption of access to or use of data or a data system could be expected to have a serious adverse effect on the University operations, assets or individuals	The disruption of access to or use of data or a data system could be expected to have a severe or catastrophic adverse effect on the University operations, assets or individuals

3.8 Appendix 2

3.8.1 Responsibilities Table

Classification	Access	Storage	Disposal
Public	Records are accessible by external parties from any location	Storage must be as per Section 4: Data Storage	Disposal must be as per *Records Management Procedure*
General Internal	Information is classified as General Internal by default unless reclassified by the creator; access to General Internal records and files is limited to University staff or other authorised personnel	Storage must be as per Section 4: Data Storage	Disposal must be as per *Records Management Procedure*
Protected	Access to records and files requires authentication and password protection. Records accessible by only a limited number of authorised people. Records and portable storage devices should be	Storage must be as per Section 4: Data Storage	Disposal must be as per *Records Management Procedure*

	stored in a secured (locked) location		
Restricted	Access to records and files requires authentication and password protection Record and file access must be protected and accessible by only senior management within the University Devices and records must be stored in a secured (locked) location	Storage must be as per Section 4: Data Storage If data is to be moved, it must be encrypted	Disposal must be as per *Records Management Procedure*

4. Data Storage

4.1 Purpose

This procedure supports and mandates the implementation of Section 2: Master Data Management and *Research Data Management Procedure*. It expands on the principles outlined in the policies as they relate to data management and provides guidance on the implementation and practical application of data storage solutions.

4.2 Scope

This procedure applies to all digital and digitised data produced, stored and/or utilised by members of the University's community.

While partner provider organisations are supported through the use of specific University information technology systems, this procedure **does not apply** to electronic data created, managed or stored by these organisations.

4.3 Legislative Context

- Federation University Australia Act 2010
- Information Privacy Act 2000 (Victoria)
- Electronic Transactions Act 2000 (Victoria)
- Public Record Act 1973 (Victoria)
- Privacy and Data Protection Act 2014
- Australian Copyright Act of 1968
- Evidence Act 1958 (Victoria)
- Australian Code for the Responsible Conduct of Research (2007)
- OECD Principles and Guidelines for Access to Research Data from Public Funding (2007)
- Australian Skills Quality Authority ASQA

- Higher Education Standards Framework (Threshold Standards) 2011
- Tertiary Education Quality and Standards Agency (TEQSA)

4.4 Definitions

A complete list of definitions relevant to this procedure is contained within Section 2: Master Data Management.

A further list of definitions **specifically** relevant to this procedure is included below:

Term	Definition
Cloud computing	The delivery of on-demand computing resources over the internet with four options in terms of access and security: **Private cloud** – services and infrastructure maintained and managed by self or a third party which reduces potential security and control risks particularly in relation to sensitive data requirements e.g. data and applications are a core part of your business **Community cloud** – several organisations with similar security considerations share access to a private cloud e.g. a group of franchises who have their own private clouds which are hosted remotely in a private environment **Public cloud** – services are stored off-site, managed by an external organisation such as Google or Microsoft and accessed over the internet which offers the greatest level of flexibility and cost saving but more vulnerable than private clouds **Hybrid cloud** – takes advantage of both public and private cloud services and gain benefits by spreading options across different cloud models e.g. use public cloud for emails to save on large storage costs while keeping highly sensitive data safe and secure behind the firewall in a private cloud
Cloud-based applications	Software as a Service (SaaS), run on cloud computers that are owned and operated by others and connect to users' computers via the internet and a web browser
Cloud-based environment	Platform as a service (PaaS) provides everything required to support the complete lifecycle of building and delivering web-based (cloud) applications, without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting
Information Security Classification	An Information Security Classification is assigned to a set of information after the creator (user) assesses the sensitivity and importance of the information. This classification determines the appropriate methods of storage and management for the information. Information Security Classifications include: **Public** – information that is publicly available and unlikely to impact on the reputation of the University, other organisation or individual e.g. academic calendar, unit outlines **General Internal** – University information that is not generally made publicly available and release of such information may cause minor impact

	on the reputation of the University, other organisation or individual e.g. academic lecture notes **Protected** – confidential University information with limited access with unauthorised disclosure, modification. Data that is released which could cause reputational harm or embarrassment to the University e.g. budget data, academic records, student grades, planning or purchasing documents **Restricted** – strictly confidential or sensitive University information restricted to individuals who are explicitly granted access with unauthorised disclosure, modification or destruction most likely to cause serious harm to the University, other organisation or individual, compromise Australia's national security, national interests, economy, stability, integrity or damage international relations or defence e.g. research requiring ethics clearances, information relating to allegations of fraud
Metadata	Describes information about data, such that data can be discovered, understood, re-used and integrated with other data; information described in a metadata record includes where and when the data was collected, created, organised, transmitted (where applicable) and last updated and who is responsible, allowing correct attribution to the creators of the work
On-premise Storage	Refers to locations inside the University network which is controlled and managed by University Information Technology Services ITS staff and remains within the University network and security infrastructure

4.5 Actions

4.5.1 Determining data storage compliance requirements

	Activity	Responsibility	Steps
A.	Checking data classification	Data Steward	1. Apply data classification scheme to determine if the data can be stored on University sanctioned cloud storage services – if not, refer Action 4.5.3: Accessing on-premise Storage
B.	Determine compliance requirements	Data Steward	1. In context of the data to be stored refer to 4.3: Legislative Context to determine the compliance requirements that apply. 2. Compare compliance requirements against provided data storage options compliance certifications.

C.	Determining suitability of cloud storage	Data Steward	1. Staffing and financial data may be stored in university sanctioned cloud services.

4.5.2 Providing data storage options

	Activity	Responsibility	Steps
A.	Protecting data	ITS	1. Provide options for the storage of digital data, including those housed on-premise and in the cloud including approved corporate business systems, network drives and approved cloud-based applications • Business information systems Use business information systems to store data that relates to a specific business function (i.e. student data should be stored in the Student Management System) • SharePoint may be used to store other types of data – refer Section 3: Data Classification and Usage • Cloud storage solutions deployed for the storage of University data must comply with all legislative requirements; may not be appropriate for all applications and classifications of data – the service must be fit for purpose and used appropriately
B.	Undertaking a risk assessment for prospective data storage	ITS	1. Ensure the cloud solution meets the legislative requirements of the Public Records Act 1973 (Victoria) and associated mandatory standards issued by PROV 2. Identify risks in the proposed cloud environment 3. Complete a Risk Assessment

4.5.3 Accessing on-premise storage

	Activity	Responsibility	Steps
A.	Storing Protected or Restricted data	Data Steward	1. Use of on-premise storage for any data classified as Protected or Restricted – Refer Section 3: Data Classification and Usage – may only be done by way of a University sanctioned business information system. NOTE: On-premise can be used to store data of any type, but the preference will be to store public data in University sanctioned cloud storage services – refer Action 4.5.1 Determining data storage compliance requirements 2. Input information into relevant on-premise business information system or storage location 3. Save with suitable data classification tags 4. Complete all metadata fields

4.5.4 Using cloud storage services

	Activity	Responsibility	Steps
A.	Accessing cloud storage services	Data Steward	1. Determine suitable storage location. 2. Save with suitable data classification tags 3. Complete all metadata fields

5. Responsibility

- Chief Operating Officer, Chief Operating Office is responsible for monitoring the implementation, outcomes and scheduled review of this procedure.
- Director, Information Technology Services is responsible for maintaining the content of this procedure as delegated by the Chief Operating Officer, Chief Operating Office.
- Manager, Enterprise Data is responsible for the administration support for the maintenance of this procedure as directed by the Director, Information Technology Services.

6. Records Management

Document Title	Location	Responsible Officer	Minimum Retention Period
Completed Risk Assessments	The University's approved records management system	Information Technology Services	7 years after administrative use has concluded
Agreements with Cloud Service	The University's approved records management system	ITS / Legal	7 years after expiry of agreement

7. Rescinded Documents

This manual replaces the following documents that have been rescinded when this Manual was issued.

- Master Data Management Policy IM1972
- Data Classification and Usage Procedure IM1974
- Data Storage Procedure IM1981

Glossary