University Procedure

Data Storage Procedure

Policy Code: IM1981

Table of Contents

Purpose

This procedure supports and mandates the implementation of the Master Data Management Policy. It expands on the principles outlined in the policy as they relate to data management and provides guidance on the implementation and practical application of data storage solutions.

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.

Legislative Context

- Federation University Australia Act 2010
- 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)

Authorised by: Deputy Vice-Chancellor (Student Support & Services) | Document Owner: Executive Director, Information Technology and Business Solutions | Original Issue: 31/08/2016 | Current Version: 31/08/2016 | Review Date: 31/08/2019 | Policy Code: IM1981

CRICOS Provider Number: 00103D

- 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

Definitions

A complete list of definitions relevant to this procedure is contained within the Master Data Management Policy.

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 eg data and applications are a core part of your business **Community cloud** – several organisations with similar security considerations share access to a private cloud eg 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 eg 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	Process whereby the creator (user) assesses the sensitivity and importance of the information and assigns a classification to the data/information so that it can be managed or stored appropriately eg **Public** – information that is publically available and unlikely to impact on the reputation of the University, other organisation or individual eg academic calendar, course outlines

Term	Definition
	General Internal – University information that is not generally made publically available and release of such information may cause minor impact on the reputation of the University, other organisation or individual eg 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 eg 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 eg research requiring ethics clearances, information relating to allegations of fraud
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

Actions

1. 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 systems** Use business systems to store data that relates to a specific business function (ie student data should be stored in the Student Management System) • **Network drives** These drives may be used to store other types of data – refer Data Classification and Usage Procedure • **Cloud storage** Solutions deployed for the storage of University data must comply with all legislative

	ACTIVITY	RESPONSIBILITY	STEPS
			requirements; may not be appropriate for all applications and classifications of data – the service must be fit for purpose and used appropriately – refer Appendix 1: list of Cloud Applications
B.	Undertaking a risk assessment for prospective data storage	ITS	1. Utilise the Data Requirements Checklist in Appendix 2 to ensure the cloud solution meets the legislative requirements of the Public Records Act 1973 (Victoria) and associated mandatory standards issued by PROV 2. Utilise the Risk Matrix in Appendix 3 to identify risks in the proposed cloud environment 3. Complete a Risk Assessment utilising the template in Appendix 4

2. Accessing on premises storage

	ACTIVITY	RESPONSIBILITY	STEPS
A.	Storing Protected or Restricted data	Data owner	1. Use On premise storage for any data classified as Protected or Restricted – Refer Data Classification and Usage procedure 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 1 2. Select local / On premise storage location 3. Save with suitable data classification tags 4. Complete all metadata fields

3. Determining cloud storage requirements

	ACTIVITY	RESPONSIBILITY	STEPS
A.	Checking data classification	Data owner	1. Apply data classification scheme to determine if the data can be stored on University sanctioned cloud storage services – if not, refer Action 2: On Premise Storage
B.	Determining suitability of cloud storage	Data owner	1. Refer Appendix 1: list of cloud based storage applications 2. Staffing and financial data is **NOT** to be stored in cloud services

4. Using cloud storage services

	ACTIVITY	RESPONSIBILITY	STEPS
A.	Accessing cloud storage services	Data owner	1. Determine suitable storage location. Refer Appendix 1: list of cloud based storage applications 2. Save with suitable data classification tags 3. Complete all metadata fields

Supporting Documents

- Master Data Management Policy
- Data Classification and Usage Procedure
- Research Data Management Policy
- Research Data Management Procedure (in draft)
- Data Backup and Recovery Procedure
- Records Management Policy
- Records Management Procedure

Forms.

- Appendix 1 Cloud Applications (DOCX 12.8kb)
- Appendix 2 Data Requirements Checklist PROV Standards (DOCX 37.1kb)
- Appendix 3 Cloud Services Use - Risk Matrix (DOCX 2587.9kb)
- Appendix 4 Risk Assessment Template (DOCX 2589.5kb)

Responsibility

- Deputy Vice-Chancellor, Student Support and Services is responsible for monitoring the implementation, outcomes and scheduled review of this procedure
- Executive Director, Information Technology and Business Solutions is responsible for maintaining the content of this procedure as delegated by the Deputy Vice-Chancellor, Student Support and Services

- Manager, Business Partnerships and Service Governance is responsible for the administration support for the maintenance of this policy as directed by the Executive Director, Information Technology and Business Solutions

Promulgation

The Data Storage Procedure will be communicated throughout the University community in the form of:

1. an Announcement Notice via FedNews and on the FedUni Policy Central's Policy Library 'Recently Approved Documents' page to alert the University-wide community of the approved Procedure;
2. distribution of e-mails to Head of School / Head of Department / University staff; and/or
3. notification to Organisational Units, Faculties, Directorates and other relevant parties
4. Training/Information Sessions

Implementation

The Data Storage Procedure will be implemented throughout the University via:

1. an Announcement Notice via FedNews and on the FedUni Policy Central's Policy Library 'Recently Approved Documents' page to alert the University-wide community of the approved Procedure;
2. Staff induction sessions
3. Training sessions, if required

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 Provider	The University's approved records management system	ITS / Legal	7 years after expiry of agreement