Data Classification and Usage Procedure

Policy Code: IM1974

Table of Contents

Purpose

Federation University Australia recognises that its corporate and research data are important strategic assets. This procedure supports and mandates the implementation of the Master Data Management Policy and Research Data Management Policy. 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.

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.

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)

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
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

Term	Definition
	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, course 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

Actions

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

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

	ACTIVITY	RESPONSIBILITY	STEPS
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. 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 the University's Data Storage Procedure
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

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 Privacy Officer 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

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

6. Using data

	ACTIVITY	RESPONSIBILITY	STEPS
A.	Ensuring data usage is appropriate	Data Steward	1. Access and use data in accordance with the Data

	ACTIVITY	RESPONSIBILITY	STEPS
			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

Supporting Documents

- Master Data Management Policy
- Data Storage Procedure
- Research Data Management Policy
- Research Data Management Procedure
- Data Backup and Recovery Procedure
- Records Management Policy
- Records Management Procedure
- Information Privacy Policy
- Information Privacy Procedure
- Information Security Policy

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 policy as directed by the Director, Information Technology and Services

Promulgation

The Data Classification and Usage 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, Schools, Directorates and other relevant parties
4. training / information sessions

Implementation

The Data Classification and Usage 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
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

Appendix 1

Data Classification Scheme

Classification	Examples	Potential Impact (refer Level of Impact Table)
Public	Newsletter, education material created for public use, course schedule, course catalogue, campus brochure, campus map, annual report, published journal article	Negligible adverse impact to the University if disclosed
General Internal	academic lecture notes, course 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

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

	Potential Impact		
Integrity Guarding against improper data modification or destruction and includes ensuring data non-repudiation and authenticity	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
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

Appendix 2

Responsibilities Table

Classification	Access	Storage	Disposal
Public	Records are accessible by external parties from any location	Storage must be as per Data Storage Procedure	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 Data Storage Procedure	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	Storage must be as per Data Storage Procedure	Disposal must be as per Records Management Procedure

Classification	Access	Storage	Disposal
	should be 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 Data Storage Procedure If data is to be moved, it must be encrypted	Disposal must be as per Records Management Procedure