Murdoch UNIVERSITY

Policy

Data Classification Policy

Purpose:	To establish awareness, direction and the compliance necessary to secure data at the University.		
Audience:	Staff, Students, Authorised visitors, Tenants of Murdoch University		
Contact Officer:	Manager Records Management and Archives	**Phone:**	See Campus Directory

Printed copies are for reference only. Please refer to the electronic copy in Policy and Procedure Manager™ [the electronic policy management system (EPMS)] to ensure you are referring to the latest version.

Preamble:

The University creates, receives, transmits and stores information that is considered sensitive and confidential. This information must be protected from loss, misuse, modification, premature destruction, and unauthorised access and/or disclosure in accordance with the University's obligations under its regulatory environment.

In concert with the University's *ICT Security Policy*, the *Data Classification Policy* observes the CIA triad information security model. This recognises Confidentiality, Integrity, and Availability of data as the key objectives of the University's information security policies. Data classification anticipates the level of impact on the University if any of these security attributes are compromised, and assists in determining the appropriate level of security and controls required for safeguarding data.

This policy establishes a data classification framework to guide data owners in determining the level of security that must be implemented to secure data and information systems based on the potential adverse impact on the University due to loss of data confidentiality, integrity, and availability.

All data should be classified into the three categories described in this policy. Security controls, appropriate to the data classification level, must then be implemented to eliminate or reduce the impact of potential risks on the University's data. In this respect, the efficient utilisation of resources is supported by focusing strategies on data sets identified in the highest risk categories.

Objectives:

This policy applies to:

1. Data, in all its forms, created, collected, processed, or stored on University equipment;
2. All staff, consultants, contractors, and organisations affiliated with the University who create, access, store or manage data relating to the University's teaching, research and administrative functions.

This policy does not apply to individually-owned data (personal information that is not relevant to University business) or data whose copyright is owned by individual staff or students.

Policy:

1. Responsibilities

The following roles and responsibilities are established for purposes of implementing this policy:

1.1. **Data Custodians** maintain physical custody of institutional data. This role is primarily managed by the Information Technology Services Office which has responsibility for the University's ICT network infrastructure and mission-critical applications. The Data Custodian is responsible for providing a secure physical and system control framework to protect data. Responsibilities also include data lifecycle management, backup and recovery processes, and managing and monitoring access privileges. They are responsible for using best practice to maintain the confidentiality, integrity and availability of information.

1.2. **Data Owners** are typically senior-level staff with authority and accountability for data sets within their functional areas. They are responsible for policy oversight and ensuring that data is evaluated and classified in accord with the data classification system outlined in this policy. They are responsible for delegating responsibilities to Data Stewards, where appropriate.

1.3. **Data Stewards** are staff with responsibility for implementing data management policies for their functional areas. They are responsible for liaising with relevant staff to determine security classifications and ensuring appropriate safeguards are implemented to protect data from unauthorised access and loss.

1.4. **Data Users** are persons authorised to access and use the University's data in order to perform their duties. Data Users are in a position of trust and are responsible for complying with relevant University policies pertaining to the use, collection, storage and sharing of data. They must abide by requirements to protect the confidentiality, privacy and integrity of data.

2. Classification Levels

All data shall be assigned one of the following three security classifications. Where data collections contain diverse data with different levels of sensitivity, the most secure classification level pertaining to any of the individual data elements should be assigned to the collection. For example, if a data collection contains both public and confidential elements, the data collection should be classified as confidential.

2.1. Highly Confidential

Data should be classified as Highly Confidential when the unauthorised disclosure, alteration or destruction of that data could cause a *significant* level of risk to the University and its affiliates.

Highly Confidential data is information that is available only to authorised persons on a legitimate need-to-know basis because of legal, privacy, commercial, contractual or other constraints. Access is dependent upon authorisation by the appropriate Data Owner or Data Steward or as required by law. Information classified as Highly Confidential has the potential to expose the University to significant risk and consequently the highest level of oversight and security controls should be applied to protect the data from unauthorised disclosure, alteration or destruction.

Where a Data Owner has not explicitly assigned another classification, Highly Confidential is the default classification for all University data and information systems.

2.2. Confidential

Data should be classified as Confidential when the unauthorised disclosure, alteration or destruction of that data could cause a *moderate* level of risk to the University and its affiliates.

Confidential data can be shared with other Offices and Schools where there is a legitimate need to access and use the data. It should generally not be disclosed outside the University without permission from the relevant Data Owner or Data Steward or as required by law.

2.3. Public

Data should be classified as Public when the unauthorised disclosure, alteration or destruction of that data would result in *little or no* risk to the University and its affiliates.

Public data is information that is typically intended for distribution outside the University and consequently may be freely shared with any person regardless of their affiliation with the University, and without the need to request authorisation from a Data Owner or Data Steward.

While little or no controls are required to protect data that is already in the public domain from disclosure, it is necessary to ensure appropriate security controls are maintained to prevent unauthorised alteration or destruction of original (source) data.

3. Security Objectives

The University's three data security objectives are:

3.1. **Confidentiality:** Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

A loss of *confidentiality* is the unauthorised disclosure of information.

Confidential information must be restricted to authorised staff on a need-to-know basis and in accord with their delegated level of responsibility. Mechanisms that control access should be proportionate to the sensitivity of the data.

3.2. **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

A loss of *integrity* is the unauthorised modification or destruction of information.

The consistency, accuracy, and trustworthiness of data must be maintained over their entire life cycle. Measures must be taken to ensure that data cannot be modified in an unauthorised or undetected manner, it cannot be deleted by unauthorised persons, and the origin of any system actions can be verified and traceable.

3.3. **Availability:** Ensuring timely and reliable access to and use of information.

A loss of availability is the disruption of access to or use of information or an information system.

Availability is ensured by such measures as implementing security controls to avoid or minimise security risks, stringent maintenance of system hardware, fast recovery processes, and minimising disruptions to service caused by system upgrades, maintenance activities and network and server outages.

4. Potential Impact if Security Objectives are compromised

There are three levels of potential impact on the University should there be a breach of a security objective, i.e. a loss of confidentiality, integrity, or availability.

4.1. Low

The potential impact is Low if the loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on the University's operations, its assets, or on individuals.

A limited adverse effect would mean that loss of confidentiality, integrity, or availability may:

(a) cause a degradation in mission capability to an extent and duration that the University is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

(b) result in minor damage to the University's assets;

(c) result in minor financial loss; or

(d) result in minor harm to individuals.

4.2. Moderate

The potential impact is Moderate if the loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on the University's operations, its assets, or on individuals.

A serious adverse effect would mean that loss of confidentiality, integrity, or availability may:

(a) cause a significant degradation in mission capability to an extent and duration that the University is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

(b) result in significant damage to the University's assets;

(c) result in significant financial loss; or

(d) result in significant harm to individuals but that does not involve the loss of life or serious threatening injuries.

4.3. High

The potential impact is High if the loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on the University's operations, its assets, or on individuals.

A severe or catastrophic adverse effect would mean that loss of confidentiality, integrity, or availability may:

(a) cause a severe degradation in or loss of mission capability to an extent and duration that the University is not able to perform one or more of its primary functions;

(b) result in major damage to the University's assets;

(c) result in major financial loss; or

(d) result in severe or catastrophic harm to individuals involving loss of life or serious threatening injuries.

Attachment 1 summarises the potential impact on the University if security objectives are compromised.

5. Common Data Elements

Attachment 2 provides examples of common data elements for each of the classification levels.

6. Enforcement

Violations of this Policy may result in disciplinary action as defined by current University policy or contract.

Supporting Procedures:

There are no supporting procedures.

Supporting Guidelines:

There are no supporting guidelines.

Supporting Standards:

There are no supporting standards.

Performance Indicators:

There are no performance indicators.

Definitions:

The definition of these terms appears in the "Dictionary of Terms". Please refer to the "Dictionary of Terms" in Policy and Procedure Manager™ to ensure you are referring to the latest version.

There are no key terms.

Related Documents:

Fraud, Corruption and Misconduct Policy

ICT Security Policy

IT Conditions of Use Policy

ICT Security Standard

Privacy Policy

Recordkeeping Policy

Research Data and Materials Recordkeeping Guideline

References:

Corruption, Crime and Misconduct Act 2003 (WA)

Criminal Code Act Compilation Act 1913 (WA)

Electronic Transactions Act 2011 (WA)

Evidence Act 1906 (WA), Acts Amendment (Evidence) Act 2000 (WA)

Freedom of Information Act 1992 (WA)

Privacy Act 1988 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

State Records Act 2000 (WA)

Approval and Implementation:

Approval Authority:	Chief Operating Officer
Responsible Officer(s):	University Secretary Director Information Technology Services

Revision History:

Version	Date Approved	Effective Date (if later than 'Date Approved')	Next Review Date	Resolution No. (if applicable)
Administrative amendments	08/03/2019			
Administrative amendment	03/04/2017			
Approved	05/07/2016		05/07/2019	